



The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency of the bid-opening process, this documentation submitted online is publicly posted by the West Virginia Purchasing Division at ***WVPurchasing.gov*** with any other vendor responses to this solicitation submitted to the Purchasing Division in hard copy format.

Header 3

List View

General Information Contact Default Values Discount Document Information Clarification Request

Procurement Folder: 1077957

Procurement Type: Central Master Agreement

Vendor ID: 000000174254

Legal Name: AUDIT SERVICES US LLC

Alias/DBA:

Total Bid: \$19.50

Response Date: 08/30/2022

Response Time: 17:59

Responded By User ID: bspannasus212

First Name: Benjamin

Last Name: Spann

Email: bspann@auditservicesus

Phone: 225-324-0139

SO Doc Code: CRFQ

SO Dept: 1300

SO Doc ID: STO2300000001

Published Date: 8/30/22

Close Date: 9/7/22

Close Time: 13:30

Status: Closed

Solicitation Description: Addendum No.4 Audit Services for Unclaimed Property

Total of Header Attachments: 3

Total of All Attachments: 3



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Solicitation Response

Proc Folder: 1077957
Solicitation Description: Addendum No.4 Audit Services for Unclaimed Property
Proc Type: Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2022-09-07 13:30	SR 1300 ESR08302200000001071	1

VENDOR
000000174254
AUDIT SERVICES US LLC

Solicitation Number: CRFQ 1300 STO2300000001
Total Bid: 19.5
Response Date: 2022-08-30
Response Time: 17:59:13
Comments:

FOR INFORMATION CONTACT THE BUYER

Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X	FEIN#	DATE
-----------------------	-------	------

All offers subject to all terms and conditions contained in this solicitation

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
1	Audit services				10.50

Comm Code	Manufacturer	Specification	Model #
84111600			

Commodity Line Comments: Affirmative.

Extended Description:

Audit/Collection of Property per section 4.1.21 of Specifications. Rate shall not exceed 10.5% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Audit services				9.00

Comm Code	Manufacturer	Specification	Model #
84111600			

Commodity Line Comments: Affirmative.

Extended Description:

Audit / Voluntary Compliance Program per section 4.2.10 of Specifications. Rate shall be flat rate of 9% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Audit services	0.00000	HOUR	100.000000	0.00

Comm Code	Manufacturer	Specification	Model #
84111600			

Commodity Line Comments: Affirmative.

Extended Description:

Audit /Other Services per section 4.3.1 of Specifications. Rate shall not exceed \$100 per hour. Vendor must enter their hourly rate and affirmation on Exhibit A Pricing Page and return with their bids.

**Response to Request
For Quotations**

**To Provide Auditing Services
for Unclaimed Property**

West Virginia State Treasurer's Office

**RFQ# STO2300000001
Opening Date: September 7, 2022**

Response Submitted By:

**Audit Services, U.S., LLC
370 Lexington Avenue
Suite 707
New York, NY 10017**



Benjamin C. Spann
Chief Executive Officer

370 Lexington Avenue, Suite 707
New York, NY 10017-6589
tel: 225.324.0139
fax: 225.753.8290
bspann@auditservicesus.com

August 25, 2022

Toby L. Welch
West Virginia Department of State Treasury
322 70th Street SE
Charleston, WV

Dear Toby:

Please find included one original electronic copy of our response to the State of West Virginia's Request for Quotation number STO2300000001 for Audit Services for Unclaimed Property. The Federal Employer Identification Number for Audit Services U.S., LLC is 31-1653187.

Audit Services U.S., LLC ("ASUS") has been in the unclaimed property auditing business for over twenty-five (25) years and our staff has performed over 10,000 audits of holders who have either failed to report unclaimed property or who have a poor reporting history. The audits our Company has performed have resulted in the identification of over \$1 billion dollars to the States and the District of Columbia. Since our inception, we have performed audits on entities, including but not limited to financial institutions, insurance companies, transfer agents, brokerage houses and other large corporations.

In 2016, Audit Services dedicated new resources to reorganize its unclaimed property auditing program, recruited expert managers and consultants, and created an expanded new compliance service offering to better serve its clients. Also included in our response is information regarding our expertise and experience in performing unclaimed property examinations. We have the knowledge and technical tools needed to provide the West Virginia Department of Treasurer's Office the resources needed to serve as an extension of their Program in the effort to recover unclaimed property for the benefit of the citizens of West Virginia.

I am the Chief Executive Officer of ASUS, and accordingly duly authorized to bind the Company to the terms of the RFQ and this response thereto. I declare that we have read the RFQ in its entirety, including all links and all Addenda released in conjunction with the RFQ. I further declare that we are knowledgeable of West Virginia's unclaimed property law and our Company complies with the minimum qualifications identified in this RFQ. My email address is bspann@auditservicesus.com and I may be reached at (225) 324-0139 should you have any questions or require additional information.

Sincerely,

A handwritten signature in blue ink that reads 'Benjamin C. Spann'.

Benjamin C. Spann
Chief Executive Officer

TABLE OF CONTENTS

Cover Page

Letter of Transmittal

Table of Contents

Designated Contact / Certification and Signature

Addendum Acknowledgements

Executive Summary

TECHNICAL PROPOSAL

3. QUALIFICATIONS

- 3.1 Knowledge**
- 3.2 Organization**
- 3.3 Location**
- 3.4 Quality Control Review**
- 3.5 Internal Controls, Security and Technology**
- 3.6 References**
- 3.7 Experience**
- 3.8 Standards**
- 3.9 Staff Qualifications**
 - 3.9.1 Experienced Staff**
 - 3.9.2 Partner & Supervisory Qualifications**
 - 3.9.3 Continuation of Quality Staff**
 - 3.9.4 Subcontractors**

4. MANDATORY REQUIREMENTS

- 4.1 Mandatory Contract Services Requirements and Deliverables**
 - 4.1.1 Specific Work Plan – Audits**
 - 4.1.2 Audits Examinations**
 - 4.1.3 Requesting Multi-State Audit Examinations**
 - 4.1.4 State Specific Audit**
 - 4.1.5 Audit Authorization**
 - 4.1.6 Multi-State Audit Authorizations**
 - 4.1.7 Authority**
 - 4.1.8 Timeframe**
 - 4.1.9 Act Requirements and Notices**

- 4.1.10 Bankruptcy of Holder**
- 4.1.11 Closure**
- 4.1.12 Reporting**
- 4.1.13 Securities**
- 4.1.14 Demands for Remittance**
- 4.1.15 Dispute Resolution**
- 4.1.16 Property Disputes**
- 4.1.17 Release Agreements**
- 4.1.18 Work-In-Progress Reports**
- 4.1.19 Review and Retention of Records**
- 4.1.20 Joint Examinations**
- 4.1.21 Fees**
- 4.1.22 Confidentiality**

4.2. ADDITIONAL OPTIONAL SERVICES WHICH VENDOR MAY PROVIDE

- 4.2.1 Additional Services**
- 4.2.2 Assistance**
- 4.2.3 Identification**
- 4.2.4 Authorization**
- 4.2.5 Contractor Assisted Self Audit**
- 4.2.6 Timeframe**
- 4.2.7 Work-In-Progress**
- 4.2.8 Collection and Delivery**
- 4.2.9 Education and Compliance**
- 4.2.10 Compensation**

4.3 ADDITIONAL SERVICES

- 4.3.1 Compensation**

5. CONTRACT AWARD

- 5.1 Contract Award**
- 5.2 Pricing Page**

6. PERFORMANCE

7. PAYMENT

8. TRAVEL

9. FACILITIES ACCESS

10. VENDOR DEFAULT

11. MISCELLANEOUS

WEST VIRGINIA EXHIBITS

West Virginia Exhibit A – Pricing Page
West Virginia Exhibit B – WV Property Type Codes
West Virginia Exhibit C – Standard Release Agreement
West Virginia Exhibit D – Work-In-Progress Report Template

AUDIT SERVICES EXHIBITS

A. Organizational Chart
B. Audit Program
C. Audit Operation Procedures Manual
D. Information Security Policy
E. Blue Hill Data Services Certification and SOC Reports
F. Microsoft Office 365 Certification and SOC Reports
G. Cross Country Computing Corporation Certification and SOC Report
H. Cyber Incident Response Plan
I. Contract States
J. Employee Resumes
K. Sample Authorization/Engagement Letter
L. Audit Services System
M. APEARS Instructions
N. Sample Global Resolution Agreement
O. Contractor Assisted Self Audit (CASA)
P. Sample Holder Profile
Q. Sample Invoice
R. Sample Work-In-Progress Report

DESIGNATED CONTACT: Vendor appoints the individual identified in this Section as the Contract Administrator and the initial point of contact for matters relating to this Contract.

(Name, Title) Benjamin C. Spann, CHIEF EXECUTIVE OFFICER
(Printed Name and Title) Benjamin C. Spann, Chief Executive Officer
(Address) 370 Lexington Avenue, Suite 707, New York, NY 10017
(Phone Number) / (Fax Number) Phone: (225) 324-0139 Cell: (212) 594-5571
(email address) bspann@auditservicesus.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through wvOASIS, I certify that: I have reviewed this Solicitation/Contract in its entirety; that I understand the requirements, terms and conditions, and other information contained herein; that this bid, offer or proposal constitutes an offer to the State that cannot be unilaterally withdrawn; that the product or service proposed meets the mandatory requirements contained in the Solicitation/Contract for that product or service, unless otherwise stated herein; that the Vendor accepts the terms and conditions contained in the Solicitation, unless otherwise stated herein; that I am submitting this bid, offer or proposal for review and consideration; that I am authorized by the vendor to execute and submit this bid, offer, or proposal, or any documents related thereto on vendor's behalf; that I am authorized to bind the vendor in a contractual relationship; and that to the best of my knowledge, the vendor has properly registered with any State agency that may require registration.

By signing below, I further certify that I understand this Contract is subject to the provisions of West Virginia Code § 5A-3-62, which automatically voids certain contract clauses that violate State law; and that pursuant to W. Va. Code 5A-3-63, the entity entering into this contract is prohibited from engaging in a boycott against Israel.

Audit Services U.S., LLC

(Company) Benjamin C. Spann, CHIEF EXECUTIVE OFFICER
(Authorized Signature) (Representative Name, Title) Benjamin C. Spann, Chief Executive Officer August 26, 2022
(Printed Name and Title of Authorized Representative) (Date)
Phone: (225) 324-0139 Fax: (212) 594-5571
(Phone Number) (Fax Number)
bspann@auditservicesus.com
(Email Address)

WVSTO

Addendum Acknowledgement Forms



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Consulting

Proc Folder: 1077957

Doc Description: Addendum No.1 Audit Services for Unclaimed Property

Reason for Modification:

Addendum No. 1 is issued to
move the bid opening date

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2022-08-11	2022-08-31 13:30	CRFQ 1300 STO2300000001	2

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 174254

Vendor Name : Audit Services U.S., LLC

Address : 370 Lexington Avenue, Suite 707

Street :

City : New York

State : NY

Country :

Zip : 10017

Principal Contact : Benjamin C. Spann

Vendor Contact Phone: (225) 324-0139

Extension:

FOR INFORMATION CONTACT THE BUYER

Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X

FEIN#

31-1653187

DATE

August 11, 2022

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

Addendum No. 1 is issued for the following reasons:

1) To move the bid opening date from 08/17/2022 to 08/31/2022.

---no other changes---

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit/Collection of Property per section 4.1.21 of Specifications. Rate shall not exceed 10% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit / Voluntary Compliance Program per section 4.2.10 of Specifications. Rate shall be flat rate of 9% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO		SHIP TO	
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE		WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Audit services	0.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit /Other Services per section 4.3.1 of Specifications. Rate shall not exceed \$100 per hour. Vendor must enter their hourly rate and affirmation on Exhibit A Pricing Page and return with their bids.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 4:00 p.m.	2022-08-10

SOLICITATION NUMBER: CRFQ STO2300000001

Addendum Number: 1

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☒ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☐ Other

Description of Modification to Solicitation:

Addendum No. 1 is issued for the following reasons:

- 1) To move the bid opening date from 08/17/2022 to 08/31/2022.

—no other changes—

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ STO23*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Audit Services U.S., LLC

Company



Authorized Signature

August 11, 2022

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Revised 6/8/2012



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Consulting

Proc Folder: 1077957

Doc Description: Addendum No.2 Audit Services for Unclaimed Property

Reason for Modification:

Addendum No. 2 is issued to publish a copy of questions with the responses and to publish a revised See Page 2 for complete info

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2022-08-15	2022-08-31 13:30	CRFQ 1300 STO2300000001	3

BID RECEIVING LOCATION

BID CLERK

DEPARTMENT OF ADMINISTRATION

PURCHASING DIVISION

2019 WASHINGTON ST E

CHARLESTON WV 25305

US

VENDOR

Vendor Customer Code: 174254

Vendor Name : Audit Services U.S., LLC

Address : 370 Lexington Avenue, Suite 707

Street :

City : New York

State : NY

Country :

Zip : 10017

Principal Contact : Benjamin C. Spann

Vendor Contact Phone: (225) 324-1039

Extension:

FOR INFORMATION CONTACT THE BUYER

Toby L Welch

(304) 558-8802

toby.l.welch@wv.gov

Vendor
Signature X

FEIN#

31-1653187

DATE

August 16, 2022

All offers subject to all terms and conditions contained in this solicitation

Reason for Modification:

Addendum No. 2 is issued to publish a copy of questions with the responses and to publish a revised Exhibit A Pricing Page

ADDITIONAL INFORMATION

Addendum No. 2 is issued for the following reasons:

1) To publish a copy of the vendor questions with responses

2) To publish a revised Exhibit A Pricing page

As per attached documentation.

—no other changes—

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit/Collection of Property per section 4.1.21 of Specifications. Rate shall not exceed 10% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit / Voluntary Compliance Program per section 4.2.10 of Specifications. Rate shall be flat rate of 9% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Audit services	0.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit /Other Services per section 4.3.1 of Specifications. Rate shall not exceed \$100 per hour. Vendor must enter their hourly rate and affirmation on Exhibit A Pricing Page and return with their bids.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 4:00 p.m.	2022-08-10

SOLICITATION NUMBER: CRFQ STO2300000001
Addendum Number: 2

The purpose of this addendum is to modify the solicitation identified as ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☐ Modify bid opening date and time
- ☐ Modify specifications of product or service being sought
- ☒ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☒ Other

Description of Modification to Solicitation:

Addendum No. 2 is issued for the following reasons:

- 1) To publish a copy of the vendor questions with responses
- 2) To publish a revised Exhibit A Pricing page

As per attached documentation.

—no other changes—

Additional Documentation: Documentation related to this Addendum (if any) has been included herewith as Attachment A and is specifically incorporated herein by reference.

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ATTACHMENT A

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ STO23*001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Audit Services U.S., LLC

Company



Authorized Signature

August 16, 2022

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Revised 6/8/2012

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Question 1: SOC Report Submission Requirements

It is understood that CRFQ Section 3 states that information concerning Vendor minimum qualifications is requested with the bid response to expedite evaluation and that CRFQ Section 3.5.6 requires a Vendor to provide SOC Reports, ISO Certification, with corresponding bridge letters. Keeping in mind the requirements of CRFQ *Instructions to Vendors Submitting Bids* Section 21 and *General Terms and Conditions* Section 31, instructing a Vendor not to submit material considered to be confidential, a trade secret, or otherwise not subject to public disclosure, please confirm if a detailed overview description of all external quality control reviews of a Vendor's work is considered acceptable for the evaluation of a vendor's bid response.

Answer 1:

The STO recognizes that some of this information may be considered sensitive information. With that thought in mind, the STO is revising the requirement to allow for the submission to be sent directly to the STO post award and will remain confidential. The revised requirement is as follows:

3.5.6 Within one month of a contract award pursuant to this solicitation, and annually thereafter, Vendor must provide American Institute of Certified Public Accountants (AICPA) SOC-1, Type 2; or SOC 2, Type 2; or ISO 27001:2013 Certification from an ANSI accredited certification body; or CSTAR Level 2 State RAMP Moderate Certification to the state with bridge letters to provide assurance that controls are operating during any intervening periods. The SOC-1, Type 2 report should cover all the requirements listed in AICPA's Statement on Standards for Attestation Engagements No. 18 (SSAE No. 18). If the requirements are not met annually, the STO will not authorize audits and may cancel participation in existing multi-state audits.

Question 2: Multi-state Audit Authorization Requirements

Upon review of the multi-state audit requirements of the CRFQ, including *Requesting Multi-state Audit Examinations* Section 4.1.3, specifically provision 4.1.3.1, as well as *Multi-state Audit Authorizations* Section 4.1.6, it is respectfully requested that STO consider the potential conflict these requirements pose to existing legal and contractual obligations of vendors and to the existing processes by which other states initiate examinations.

For example, by law in several states the fact of an examination and/or the identity of the holder under examination is confidential; in other states, such information is confidential by contract. In either instance, the participation of the state in the examination cannot be revealed by the auditor when inviting or soliciting another state(s) to join. Most states have their own processes and procedures for initiating audits as well as deadlines to begin

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

the examination, including West Virginia's requirement for initiating an audit within 90 days under CRFQ Section 4.1.8.

In our experience, most states send the notice of audit letters to the holder directly and not through the auditor, so the auditor generally will not be able to collect letters from all participating states to forward together to initiate an audit. In addition, because states have different timelines for deciding whether to join audits, waiting until all states have joined may extend the start of an examination beyond the state's deadline. With these considerations in mind, will the STO consider amending these specific requirements that impact the rights of other states in a multi-state audit, allowing a vendor to appropriately serve the STO, while also adhering to all existing laws, contractual obligations, and processes associated with performing multi-state audits?

Answer 2:

STO agrees to amend the following requirements for the two (2) sections of the specification to ensure that the vendor will not have any legal or contractual conflicts with other vendors as well as other conflicts.

4.1.3 Requesting Multi-State Audit Examinations: Prior to the commencement of any audit, Vendor shall draft and submit electronically, to the Unclaimed Property Compliance Director, a request for audit. The request for audit should include the following information, if available. The auditor is not required to submit information regarding another state if confidential by law or by contract. Failure to provide sufficient information may result in the rejection of the audit.

4.1.6 Multi-state Audit Authorizations: In the event of multi-state audits, and if in agreement with some or all participating states, Vendor will request and receive approval from a majority of participating states prior to initiation of the audit, if possible. The authorization letters will be sent in a single batch or minimal batches from all states that are in agreement with this process to serve as notice to the Holder of the initiation of the multi-state audit and as a signal of uniformity by the participating states.

Question 3: Identification and Collection Fees

It is understood that CRFQ Section 4.1.21.1 requires all vendor fees for the identification and collection of unclaimed property to be the lesser of a flat 10 percent (10%) of the net unclaimed property remitted to STO or the lowest fee percentage charged to any other state for the same holder multi-state audit.

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Upon review of this fee requirement, along with the qualifications and mandatory requirements of the CRFQ, it is respectfully requested that the STO consider the overall cost of providing the audit services sought, including the financial obligations to maintain the professional and technical resources required to provide professional auditing services of the highest quality and standards, the fees incurred to provide short-term custody services of remitted unclaimed property from holders, the expense of procuring the necessary professional and cyber security insurance, the cost of hiring external third-party auditors to perform required quality control reviews, as well as the rising costs of doing business in today's economy. With these factors in mind, would the STO consider increasing the cap on the fee percentage by less than 1% for the identification and collection of unclaimed property?

Answer 3:

The fee per Section 4.1.21 is a flat 10% or the lowest fee charged by any other state, whichever rate is lower. See Section 4.1.21 of the RFQ for the complete language and there is no update to this section.

Question 4: STO Requested and Approved Services – Bid Requirements

Upon review of the requested and approved services of the CRFQ, it is noted that there are three distinct commodity line items under this solicitation for bids:

- 1) Audit/Collection of Property per Specifications Section 4.1.21,
- 2) Audit/Voluntary Compliance Program per Specifications Section 4.2.10, and
- 3) Audit/Other Services per Specifications Section 4.3.1.

Would the STO please clarify if a Vendor must bid on all three commodity line items to be considered for contract award? Alternatively, if a Vendor does not wish to participate in the provision of services for certain commodity line items of the solicitation may a Vendor indicate that it “does not wish to participate in...” for one or more of the commodity line items when responding to *Mandatory Requirements* Section 4 and when completing *Exhibit A – Pricing Page* of the CRFQ?

Answer 4:

The Vendor is required to bid on the mandatory services, per Section 4.1.21.

The Vendor is not required to bid on the optional services, per Section 4.2.10 and 4.3.1. See revised Exhibit A Pricing Page.

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Question 5: In the CRFQ, Section 3.5 Internal Controls, Security and Technology (pages 29 and 30 of 48), there is a list of requirements. These are numbered as 3.5.1-3.5.4 and 3.5.6. There is no 3.5.5. Is this a numbering anomaly or is requirement 3.5.5 missing from this section?

Answer 5:

Section 3.5.5 is a numbering anomaly – no section exists. In addition, Section 3.54 should read as 3.5.4.

Question 6: In the CRFQ, in Section 5: Contract Award, 5.2 Pricing Page (pages 39 and 40 of 48), it states:

"Vendor should complete the Pricing Page (Exhibit A) by affirming it accepts the set reimbursement fees listed in subsections 4.1.21, 4.2.10, and 4.3.1. Vendor should complete the Pricing Page in full as failure to complete the Pricing Page in its entirety may result in Vendor's bid being disqualified."

Is the vendor permitted to bid on only the unclaimed property auditing services (Per Section 4.1.21) and thereby decline to bid on the Voluntary Compliance Program and the hourly rate services? Alternatively, is the bidder required to bid on all three service types?

Answer 6:

Vendor is permitted to bid on only the unclaimed property auditing services, mandatory service, per Section 4.1.21. See response to Question 4 and revised Exhibit A Pricing Page.

Question 7: Please confirm that the fees outlined in Exhibit A – Pricing Page would be prospective only for newly commenced audits and audits commenced under the current contract would be compensated according to the pricing schedule at the time the audit was authorized.

Answer 7:

Correct. The fees in Exhibit A will be effective for newly commenced audits. These audits will be identified by an audit authorization letter dated after a new contract period begins.

Question 8: Please confirm that type of response you are looking for on Exhibit A – Pricing Page in the blank space before "affirmation" – a signature, initials, other?

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Answer 8:

See revised Exhibit A Pricing Page. Vendor will only need to mark 'Yes' or 'No' for the Optional Services items if they are choosing to offer those services.

Question 9: Please confirm that proposals may be submitted in *wvOASIS*.

Answer 9:

The preferred method to submit bid responses is online at wvOASIS.gov. Other methods include physical delivery, etc. See Section/item 6 Bid Submission, Instructions to Vendors Submitting Bids document for additional information.

Question 10: Section 4.1.6 states that the vendor shall request and receive approval from all participating states prior to initiation of the audit. As each state has its own authorization and audit commencement requirements and most states send authorization letters directly to the holders, we suggest that the language be amended to state that the Vendor will make its best efforts to limit the number of times audit authorization letters are sent from a Vendor to the Holder for those authorizations that are not sent directly by a participating state.

Answer 10:

This response is consistent with the answer to Question 2. The section is amended as follows:

4.1.6 Multi-state Audit Authorizations: In the event of multi-state audits, and if in agreement with some or all participating states, Vendor will request and receive approval from a majority of participating states prior to initiation of the audit, if possible. The authorization letters will be sent in a single batch or minimal batches from all states that are in agreement with this process to serve as notice to the Holder of the initiation of the multi-state audit and as a sign of uniformity by the participating states.

Question 11: In section 4.1.8 Timeframe, the RFP states that audits are authorized for two years, with not more than one (1) year extension unless there are extenuating circumstances. We request that the initial period be extended to three years, as many large-scale multi-state audits take at least that long to complete.

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Answer 11:

WV will amend section 4.1.8 Timeframe to authorize audits for three (3) years. The amended section, second paragraph, will now read as follows:

Audits shall be authorized for three (3) years from the date of the authorization letter. Should the auditor not complete the audit in that time, they shall request an extension of the audit. Extensions may be granted in one (1) year increments. If an extension is not received at least forty-five (45) days prior to the expiration of the audit, the extension request may not be reviewed, and the audit will set to expire. Unless extenuating circumstances are adequately demonstrated, no more than one (1) extension may be granted under any audit.

Question 12: Is the bidder permitted to submit a redacted version of their solicitation? There are items that are confidential in nature, but key to our response for this solicitation. Perhaps better said, if a page is marked as "Confidential", will it be treated as such?

Answer 12:

Please see response to Question 1. If additional information is required from the Vendor to complete an evaluation, and/or assign audits, the STO will permit submission of information that is especially sensitive in nature for review in determining whether the information meets specific requirements at a later date, per item 22 of Instructions to Vendors Submitting Bids document.

Question 13: Is the bidder permitted to submit their response to this solicitation by way of email to the address indicated in the solicitation (Toby.L.Welch@wv.gov)? This would be in lieu of submitting on the WV Oasis website. If the preferred method of submission is through the WV Oasis website, that is not a problem.

Answer 13:

Submission within the WV OASIS website portal is the preferred method. Bid responses will not be accepted via email per Section/item 6 of the Instructions to Vendors Submitting Bids document.

CRFQ STO2300000001
AUDIT SERVICES FOR UNCLAIMED PROPERTY
Vendor Questions

Question 14: With regards to the references requested (Section 3.6), does the State require a written response from the reference, or will just their contact information suffice?

Answer 14:

A written response from the reference is not required to be submitted with your response. However, the vendor must provide names of at least three (3) governmental agencies, which includes a contact name, phone number and type of audit services performed for the reference. The STO reserves the right to contact any person or entity it believes is prudent to inquire about the vendor.

REQUEST FOR QUOTATION
Professional Auditing Services

EXHIBIT A – PRICING PAGE (Revised)

Vendor affirms by their signature or submission of a bid response that they will accept the fee schedule as listed for all STO requested and approved services. All vendor expenses must be included in the established fee schedule and shall not be reimbursed separately.

Note: Vendor is not required to provide services considered Optional. Such response will have no bearing on a contract award.

MANDATORY SERVICES:

Per Section 4.1.21: Vendor fees for the identification and collection of unclaimed property will be a flat 10 percent (10%) of the net unclaimed property remitted to the STO, or the lowest fee percentage charged to any other state for the same Holder multi-state audit, less any interest due pursuant to the provision of this RFQ. In such case, the fee is lower than 10%, Vendor shall provide written notice of the lower fee and agree to provide the same fee.

OPTIONAL SERVICES (Non-mandatory):

Per Section 4.2.10: Compensation: All Vendor fees for the Voluntary Compliance Program will be a flat 9 percent (9%) of the net unclaimed property remitted to the STO. Net unclaimed property is the gross value of all unclaimed property, minus the value of all unclaimed property delivered by the Holder, if any, that otherwise would have been delivered pursuant to the reporting practices of the Holder as they existed prior to the execution of the agreement with Vendor.

Fee: Flat Rate of 9%

Vendor will offer this service: Yes _____ No _____

Per Section 4.3.1: Compensation: Audit Agreed Upon Procedures related to a Holder which is outside of the scope of a multistate audit, West Virginia state specific audit, or Vendor-assisted self-audits will be paid on an hourly basis at the rate of \$100 per hour, and the total cost will be capped in a release order, if selected.

Fee: Not to Exceed \$100/hour

Vendor will offer this service: Yes _____ No _____

REQUEST FOR QUOTATION
Professional Auditing Services

I/We agree to the established fee schedule for the mandatory services listed within this solicitation and resultant contract award, including any of the selected optional services affirmed above:

Company Name: _____

Printed Name of Signatory: _____

Title of Signatory: _____

Signature: _____



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Consulting

Proc Folder: 1077957

Doc Description: Addendum No.3 Audit Services for Unclaimed Property

Reason for Modification:

Addendum No 3 is issued to
modify the bid opening date and
publish a revised pricing sheet

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2022-08-23	2022-09-07 13:30	CRFQ 1300 STO2300000001	4

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 174254
Vendor Name : Audit Services U.S., LLC
Address : 370 Lexington Avenue, Suite 707
Street :
City : New York
State : NY Country : Zip : 10017
Principal Contact : Benjamin C. Spann
Vendor Contact Phone: (225) 324-0139 Extension:

FOR INFORMATION CONTACT THE BUYER

Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X

FEIN#

31-1653187

DATE August 23, 2022

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

Addendum No. 3 is issued for the following reasons:

- 1) To revise the bid opening date from 8/31/22 to 9/7/22
- 2) To publish a revised Exhibit A Pricing page
- 3) To publish a modifications to the specifications - Section 4.1.21 (Fees)

As per attached documentation.

—no other changes—

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit/Collection of Property per section 4.1.21 of Specifications. Rate shall not exceed 10% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit / Voluntary Compliance Program per section 4.2.10 of Specifications. Rate shall be flat rate of 9% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Audit services	0.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit /Other Services per section 4.3.1 of Specifications. Rate shall not exceed \$100 per hour. Vendor must enter their hourly rate and affirmation on Exhibit A Pricing Page and return with their bids.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 4:00 p.m.	2022-08-10

SOLICITATION NUMBER: CRFQ STO2300000001

Addendum Number: 03

The purpose of this addendum is to modify the solicitation identified as CRFQ STO2300000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☒ Modify bid opening date and time (*See Below*)
- ☒ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☒ Other

- 1) Revise Bid Opening Date/Time – September 7, 2022 at 1:30pm EST**
- 2) To publish a revised Exhibit A Pricing Page**
- 3) To publish a modification to the Specifications, Section 4.1.21 - Fees**

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ STO2300000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

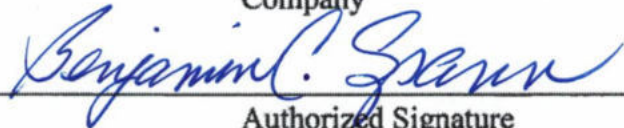
(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input checked="" type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Audit Services U.S., LLC

Company



Authorized Signature

August 23, 2022

Date

NOTE: This addendum acknowledgment should be submitted with the bid to expedite document processing.

Agency Modification to Specifications
Solicitation # CRFQ STO2100000001
ADDENDUM #03

Regarding a question received that was a part of Addendum #02 (question #3) regarding the set pricing as required per Section 4.1.21: After further review and research, the Agency wishes to modify the specification as follows:

Section 4.1.21.1 Except as provided in Section 4.2.10 and Section 4.3.1 below, all Vendor fees for the identification and collection of unclaimed property will be the lesser of a flat 10.5 percent (10.5%) of the net unclaimed property remitted to the STO, or the lowest fee percentage charged to any other state for the same Holder multi-state audit, less any interest due pursuant to the provision of this RFQ. In such case, if the fee is lower than 10.5%, Vendor shall provide written notice of the lower fee and agree to provide the same fee.

The Price Sheet is also modified to reflect the change above as well, and attached to this Addendum.

REQUEST FOR QUOTATION
Professional Auditing Services

EXHIBIT A – PRICING PAGE (Revised)

Vendor affirms by their signature or submission of a bid response that they will accept the fee schedule as listed for all STO requested and approved services. All vendor expenses must be included in the established fee schedule and shall not be reimbursed separately.

Note: Vendor is not required to provide services considered Optional. Such response will have no bearing on a contract award.

MANDATORY SERVICES:

Per Section 4.1.21: Vendor fees for the identification and collection of unclaimed property will be a flat 10.5 percent (10.5%) of the net unclaimed property remitted to the STO, or the lowest fee percentage charged to any other state for the same Holder multi-state audit, less any interest due pursuant to the provision of this RFQ. In such case, the fee is lower than 10.5%, Vendor shall provide written notice of the lower fee and agree to provide the same fee.

OPTIONAL SERVICES (Non-mandatory):

Per Section 4.2.10: Compensation: All Vendor fees for the Voluntary Compliance Program will be a flat 9 percent (9%) of the net unclaimed property remitted to the STO. Net unclaimed property is the gross value of all unclaimed property, minus the value of all unclaimed property delivered by the Holder, if any, that otherwise would have been delivered pursuant to the reporting practices of the Holder as they existed prior to the execution of the agreement with Vendor.

Fee: Flat Rate of 9%

Vendor will offer this service: Yes _____ No _____

Per Section 4.3.1: Compensation: Audit Agreed Upon Procedures related to a Holder which is outside of the scope of a multistate audit, West Virginia state specific audit, or Vendor-assisted self-audits will be paid on an hourly basis at the rate of \$100 per hour, and the total cost will be capped in a release order, if selected.

Fee: Not to Exceed \$100/hour

Vendor will offer this service: Yes _____ No _____

REQUEST FOR QUOTATION
Professional Auditing Services

I/We agree to the established fee schedule for the mandatory services listed within this solicitation and resultant contract award, including any of the selected optional services affirmed above:

Company Name: _____

Printed Name of Signatory: _____

Title of Signatory: _____

Signature: _____



Department of Administration
Purchasing Division
2019 Washington Street East
Post Office Box 50130
Charleston, WV 25305-0130

State of West Virginia
Centralized Request for Quote
Consulting

Proc Folder: 1077957

Doc Description: Addendum No.4 Audit Services for Unclaimed Property

Reason for Modification:

Addendum No 4 is issued to
correct an error

Proc Type: Central Master Agreement

Date Issued	Solicitation Closes	Solicitation No	Version
2022-08-30	2022-09-07 13:30	CRFQ 1300 STO2300000001	5

BID RECEIVING LOCATION

BID CLERK
DEPARTMENT OF ADMINISTRATION
PURCHASING DIVISION
2019 WASHINGTON ST E
CHARLESTON WV 25305
US

VENDOR

Vendor Customer Code: 174254

Vendor Name : Audit Services U.S., LLC

Address : 370 Lexington Avenue, Suite 707

Street :

City : New York

State : NY Country : USA Zip : 10017

Principal Contact : Benjamin C. Spann

Vendor Contact Phone: (225) 324-0139 Extension:

FOR INFORMATION CONTACT THE BUYER

Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor
Signature X  FEIN# 31-1653187

DATE August 30, 2022

All offers subject to all terms and conditions contained in this solicitation

ADDITIONAL INFORMATION

Addendum No. 4 is issued for the following reasons:

- 1) To correct an error from Addendum No. 3
- 2) To publish a revised Exhibit A Pricing page
- 3) To publish a modifications to the specifications - Section 4.1.21 (Fees)

As per attached documentation.

—no other changes—

INVOICE TO

WEST VIRGINIA STATE
TREASURERS OFFICE
322 70TH ST SE

CHARLESTON
US

WV

SHIP TO

WEST VIRGINIA STATE
TREASURERS OFFICE
322 70TH ST SE

CHARLESTON
US

WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit/Collection of Property per section 4.1.21 of Specifications. Rate shall not exceed 10.5% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO

WEST VIRGINIA STATE
TREASURERS OFFICE
322 70TH ST SE

CHARLESTON
US

WV

SHIP TO

WEST VIRGINIA STATE
TREASURERS OFFICE
322 70TH ST SE

CHARLESTON
US

WV

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Audit services				

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit / Voluntary Compliance Program per section 4.2.10 of Specifications. Rate shall be flat rate of 9% Vendor must enter their percentage and affirmation on Exhibit A Pricing Page and return with their bids.

INVOICE TO				SHIP TO			
WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE				WEST VIRGINIA STATE TREASURERS OFFICE 322 70TH ST SE			
CHARLESTON		WV		CHARLESTON		WV	
US				US			

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Audit services	0.00000	HOUR		

Comm Code	Manufacturer	Specification	Model #
84111600			

Extended Description:

Audit /Other Services per section 4.3.1 of Specifications. Rate shall not exceed \$100 per hour. Vendor must enter their hourly rate and affirmation on Exhibit A Pricing Page and return with their bids.

SCHEDULE OF EVENTS

<u>Line</u>	<u>Event</u>	<u>Event Date</u>
1	Questions are due by 4:00 p.m.	2022-08-10

SOLICITATION NUMBER: CRFQ STO2300000001

Addendum Number: 04

The purpose of this addendum is to modify the solicitation identified as CRFQ STO2300000001 ("Solicitation") to reflect the change(s) identified and described below.

Applicable Addendum Category:

- ☐ Modify bid opening date and time
- ☒ Modify specifications of product or service being sought
- ☐ Attachment of vendor questions and responses
- ☐ Attachment of pre-bid sign-in sheet
- ☐ Correction of error
- ☒ Other

1) To publish a revised Exhibit A Pricing Page (Rev 8/30/22)

2) To publish a modification to the Specifications, Section 4.1.21 - Fees

Terms and Conditions:

1. All provisions of the Solicitation and other addenda not modified herein shall remain in full force and effect.
2. Vendor should acknowledge receipt of all addenda issued for this Solicitation by completing an Addendum Acknowledgment, a copy of which is included herewith. Failure to acknowledge addenda may result in bid disqualification. The addendum acknowledgement should be submitted with the bid to expedite document processing.

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ STO2300000001

Instructions: Please acknowledge receipt of all addenda issued with this solicitation by completing this addendum acknowledgment form. Check the box next to each addendum received and sign below. Failure to acknowledge addenda may result in bid disqualification.

Acknowledgment: I hereby acknowledge receipt of the following addenda and have made the necessary revisions to my proposal, plans and/or specification, etc.

Addendum Numbers Received:

(Check the box next to each addendum received)

<input checked="" type="checkbox"/> Addendum No. 1	<input type="checkbox"/> Addendum No. 6
<input checked="" type="checkbox"/> Addendum No. 2	<input type="checkbox"/> Addendum No. 7
<input checked="" type="checkbox"/> Addendum No. 3	<input type="checkbox"/> Addendum No. 8
<input checked="" type="checkbox"/> Addendum No. 4	<input type="checkbox"/> Addendum No. 9
<input type="checkbox"/> Addendum No. 5	<input type="checkbox"/> Addendum No. 10

I understand that failure to confirm the receipt of addenda may be cause for rejection of this bid. I further understand that that any verbal representation made or assumed to be made during any oral discussion held between Vendor's representatives and any state personnel is not binding. Only the information issued in writing and added to the specifications by an official addendum is binding.

Audit Services U.S., LLC

Company



Authorized Signature

August 30, 2022

Date

NOTE: This addendum acknowledgement should be submitted with the bid to expedite document processing.

Agency Modification to Specifications
Solicitation # CRFQ STO2300000001
ADDENDUM #04

Regarding a question received that was a part of Addendum #02 (question #3) regarding the set pricing as required per Section 4.1.21: After further review and research, the **Agency wishes to modify the specification as follows – and correct Addendum #03:**

Section 4.1.21.1 Except as provided in Section 4.2.10 and Section 4.3.1, all Vendor fees for the identification and collection of unclaimed property will be a flat **10.5 percent (10.5%)** of the net unclaimed property remitted to the WV STO.

The Price Sheet is also modified to reflect the change above as well and attached to this Addendum.

REQUEST FOR QUOTATION
Professional Auditing Services

EXHIBIT A – PRICING PAGE (Revised 8/30/22)

Vendor affirms by their signature or submission of a bid response that they will accept the fee schedule as listed for all STO mandatory, requested and approved services. All vendor expenses must be included in the established fee schedule and shall not be reimbursed separately.

Note: Vendor is not required to provide services considered Optional. Such response will have no bearing on a contract award.

MANDATORY SERVICES:

Per Section 4.1.21.1: Vendor fees for the identification and collection of unclaimed property will be a flat 10.5 percent (10.5%) of the net unclaimed property remitted to the WV STO.

OPTIONAL SERVICES (Non-mandatory):

Per Section 4.2.10: Compensation: All Vendor fees for the Voluntary Compliance Program will be a flat 9 percent (9%) of the net unclaimed property remitted to the STO. Net unclaimed property is the gross value of all unclaimed property, minus the value of all unclaimed property delivered by the Holder, if any, that otherwise would have been delivered pursuant to the reporting practices of the Holder as they existed prior to the execution of the agreement with Vendor.

Fee: Flat Rate of 9%

Vendor will offer this service: Yes _____ No _____

Per Section 4.3.1: Compensation: Audit Agreed Upon Procedures related to a Holder which is outside of the scope of a multistate audit, West Virginia state specific audit, or Vendor-assisted self-audits will be paid on an hourly basis at the rate of \$100 per hour, and the total cost will be capped in a release order, if selected.

Fee: Not to Exceed \$100/hour

Vendor will offer this service: Yes _____ No _____

REQUEST FOR QUOTATION
Professional Auditing Services

I/We agree to the established fee schedule for the mandatory services listed within this solicitation and resultant contract award, including any of the selected optional services affirmed above:

Company Name: _____

Printed Name of Signatory: _____

Title of Signatory: _____

Signature: _____

Executive Summary

Audit Services, U.S., LLC (“**ASUS**”) is pleased to submit this response to the State of West Virginia Treasury Department, (“**State**”) for Unclaimed Property Auditing Services. This Executive Summary is intended to demonstrate that **ASUS** has the capability to provide the State with the quality of services they expect and are seeking through a contract vendor.

Recognizing that each state and the District of Columbia may approach unclaimed property auditing slightly differently, **ASUS** has developed three customizable variations of its unclaimed property auditing program to support the identification and collection of unclaimed property. In each case, the State can elect to participate and authorize audits under any or all of the different programs. The **ASUS** unclaimed property auditing programs include:

1. Comprehensive General Ledger Audits
2. Securities Compliance Audits
3. Contractor Assisted Self Audits (**CASA**)

Founded in 1997, our team is comprised of highly experienced subject matter experts, including thought leaders on general ledger auditing and analytics, unclaimed property law and litigation, and securities compliance. Most of our employees have over twenty (20) years of unclaimed property experience and are made up of many former state administrators, audit supervisors, attorneys, as well as private sector unclaimed property industry veterans. **ASUS** has the expertise, experience, skills and knowledge to identify and recover unclaimed property belonging to the citizens of the State of West Virginia. If awarded this contract, the resources expended by **ASUS** will be focused on serving as directed by the West Virginia Unclaimed Property Program.

The advantages of entering into a contract with **ASUS** include:

1. A company that conducts onsite and offsite audits, approved by the State, on entities of all sizes using our own staff comprised of a team of highly experienced auditors. Our employees were selected not only for their superior unclaimed property and accounting credentials, but also for their varied business and government experience. In addition, they are trained in all phases of

State unclaimed and abandoned property law, Supreme Court case law, Uniform Unclaimed Property Act, auditing conduct and ethics, the National Association of State Treasurers (NAST), and the National Association of Unclaimed Property Administrators (NAUPA) resolutions and commitments on how to conduct audits specifically for unclaimed and abandoned property.

2. A staff that has knowledge and experience in the unclaimed property industry, including personnel who have served in various capacities with their State Unclaimed Property Programs, as well as individuals who have worked extensively in the field of unclaimed property in the private sector. Currently, **ASUS** has contracts with forty-four (44) States and the District of Columbia. Additionally, **ASUS** presently supports West Virginia as an authorized state service provider. As such, we are directly experienced in working with West Virginia and complying with its contractual and statutory requirements.
3. The *Audit Services System* that provides the processing which produces client reports to state unclaimed property departments. Our processing software stands alone and is designed for the specific purpose of processing unclaimed property data for compliance reporting and is compatible for each State utilizing the NAUPA standard format, as well as all other proprietary formats. As such we do not require interface with any other vendors or software in the course of providing our services. The Audit Services System is on a server located in an offsite data center in Pearl River, New York and it operates on an AS400 platform. Previous unclaimed property reports utilizing this software that **ASUS** has submitted to the State has already demonstrated that this system meets the State's requirements.
4. Our commitment to:
 - *Assisting our clients* in developing sound audit and/or compliance programs to bring holders into compliance. If requested by the State, our audit team will conduct additional comprehensive audits of holders that may be too time consuming for the State's staff.
 - *Reporting names and addresses of owners* whenever records are available and utilizing sampling and extrapolation techniques only when supporting records cannot be provided.
 - *Assisting the holders* by bringing them into compliance with the State's unclaimed property law. Holders will be informed of their reporting and due diligence obligations, as well as current State laws on property classifications, dormancy periods, and service charges. They will also be informed of electronic reporting opportunities and the State's standards for filing timely reports. As part of our audit process, we recommend to the holder internal accounting controls for the reporting of unclaimed and abandoned property.

- *Assisting and sharing* our experience and knowledge of the administrative and audit process with the State's Unclaimed Property Program. Our experience and background in this specialized field qualifies our Company to serve as an extension of the Program's staff.
 - *Utilizing an audit approach that is non-controversial and non-aggressive* to the business community. We are sensitive to the concerns of the holder when conducting an audit.
 - *Remitting Property* to the State in a timely manner once it is recovered from the holder. Once the property is recovered, it will be held in a qualified custodial institution for remittance to the State.
5. Access to experienced and professional individuals who not only have extensive knowledge of the State unclaimed and abandoned property laws but the necessary skills that can provide the State with the assurance that work will be done timely and accurately. This is accomplished by utilizing the following measures:
- Developing a working relationship with the States and the holder community. The staff of **ASUS** has extensive experience in working with staff and State administrators of State unclaimed property offices across the nation, as well as all management levels of numerous corporations.
 - Being aware of the concerns of the various States, the holders and the industry representatives, and responding accordingly when conducting an examination.
6. A Company that in the conduct of its audits adheres to a policy of operating in a manner that is consistent with Generally Accepted Accounting Principles, and Generally Accepted Auditing Standards. As a result, we can provide our services with the utmost confidence. These services include, but are not limited to:
- Identifying and locating unclaimed property from the books and records of the holders and making demand pursuant to the State's procedures.
 - Providing release agreements when requested, identifying the property records to be submitted, and signed by the holder and the State.
 - Submitting reports of unclaimed property to the State in a timely manner in a format suitable to the State.
 - Submitting itemized monthly statements of unclaimed property disbursed to the State.

- Remitting property to the State within 30 days after it has been received and reconciled.
 - Instructing holders to register securities and electronically transfer to the State's custodian bank and providing them with training opportunities.
 - Notifying the holder of its continuing obligation to report unclaimed property to the State after completion of the audit.
7. A Company that holds to the findings of the U.S. Supreme Court in Texas v. New Jersey, 85 S. Ct. 1136, (1965), Pennsylvania v. New York, 92 S. Ct. 2880, (1972), and Delaware v. New York, 113 S. Ct. 1550 (1993), and any applicable federal legislation regarding which State has the right to receive unclaimed and abandoned property.
- Where the name and last known address of the apparent owner according to the books and records of the holder is in the State, it shall be deemed reportable to the State.
 - If the holder has never maintained records setting forth the name and last known address of the apparent owner, the property shall be deemed as reportable to the State of incorporation of the holder. An address shall be deemed to mean a description of location sufficient for the delivery and receipt of mail. Where no address exists, but the records of the holder establish that the apparent owner resided in State, the State and the holder's state of incorporation will be advised for the purpose of determining which state possesses the priority claim to the funds. **ASUS** will seek approval from our contract States when utilizing estimation techniques.
 - Where the address of the apparent owner cannot be readily ascertained, but in fact exists in the books and records of the holder, sampling techniques will be used to allocate the property among the states participating in the review. In such event, if required, sampling techniques will also be utilized to ascertain the proportion of the total reportable property for which the holder has names and last known addresses.
 - **ASUS** will assure that the holder has complied with the due diligence requirements of the State's statutes with respect to attempting to locate the owner of the property prior to remitting it to the State.
8. A Company that recognizes that the states it serves govern its actions, and it has the responsibility to follow the instructions of the client State for the various services provided, as well as complies with all federal, state and local laws that may apply. We are cognizant of the concerns of the States in matters dealing with potential conflicts of interest, and we hold ourselves to the highest AICPA Professional Standards to avoid such conflicts. In addition, we also certify that **ASUS** has no

conflict of interest in the conduct of any of our audits. Under no circumstance does **ASUS** represent both the holder and the States or charge a fee to both the holder and the States. All work performed will be done in accordance with the State's Unclaimed Property Law.

- 3. Qualifications:** ASUS, or ASUS's staff if requirements are inherently limited to individuals rather than corporate entities, shall have the following minimum qualifications. ASUS shall have the following minimum qualifications. Information is requested with the bid response to expediate evaluation; however, ASUS must provide requested information within two (2) business days of request.

3.1 Knowledge: Audit Services U.S., LLC, ("ASUS") has sufficient knowledge of the *West Virginia Unclaimed Property Act* (the "Act"), set forth in W.VA. Code §36-8-1, et seq., court rulings regarding the Act, and its regulations. ASUS will comply with the Act and correctly apply the law to the Holder examination. As an unclaimed property auditing services provider to West Virginia for over twenty-two (22) years, ASUS has successfully completed hundreds of audits on behalf of and reported over \$4.1 million to the state in the past ten (10) years. We believe that the combination of our highly experienced personnel, with our proven track record in West Virginia, ASUS demonstrates its knowledge, ability and commitment to comply with West Virginia's unclaimed property law, and all federal legislation and court rulings regarding the Uniform Unclaimed Property Act.

3.2 Organization: ASUS currently operates with a staff of twelve (12) professional employees which includes two attorneys. Our staff members will support the requirements involving services such as holder research, auditing, information systems support, invoicing, etc.

Our auditors are selectively recruited, trained, and dedicated to the task of completing accurate and efficient unclaimed property audits on behalf of our clients. We hold our team accountable through multiple layers of management, supervision, mentoring, and review of finished work products support the work of each of our field auditors, and ensure that all of our audit processes, findings, and documentation are followed, accurate and representative of the highest professional standards.

All current state unclaimed property auditing initiatives are led by Jeremy Katz, a nationally known unclaimed property professional with over twenty-five (25) years of experience working on behalf of all of the states. Jeremy's detailed unclaimed property experience are set forth below along the qualifications and experience of the unclaimed property team available for assignment to manage the present contract and perform the ongoing holder examination reporting, and collections tasks to be performed under the Request for Quotation.

A company organizational chart (which can be found under *ASUS Exhibit A – Organizational Chart*) illustrates the team assigned to the identification, examination and collection of unclaimed property from holders on behalf of ASUS State clients. The activities, hours allocated, and costs associated with the operation of the audit organization are coordinated in several weekly staff meetings, as well as by using electronic cloud-based contact, recordkeeping and management tools.

All operations, custody and reporting matters are managed out of our New York City based headquarters and are led by Matthew Thornton. Matthew's detailed experience is set forth below in Section 3.9.1. Matters relating to audits, contract compliance or other matters relating to supporting West Virginia may be addressed to Jeremy, Matthew or Benjamin Spann (whose biography is also set forth below). Lastly, ASUS believes in working closely with its client's states and is routinely in directly contact via email, phone and in person meetings as requested.

3.3 Location: ASUS is headquartered at 370 Lexington Avenue, Suite 707, New York, New York 10017 and all work pertaining to this RFQ will be managed out of this office. Our only business is conducting unclaimed property audits on behalf of our contract states. ASUS is authorized to conduct business in the state of West Virginia. All ASUS systems stores, processes and maintains data for the State, or a third-party under audit, within the continental United States.

3.4 Quality Control Review: ASUS maintains detailed policies and procedures regarding its operation, data security and its audit process. These policies and procedures, which include ASUS' service providers for systems, social security death master file matching and hosting of the ASUS data server, are reviewed and tested annually. Those certifications and review information are available upon request. The ASUS policies and procedures and the related reviews and certifications for ASUS and its service providers are set forth as follows:

- Audit Program – *ASUS Exhibit B*
- Audit Operation Procedures Manual – *ASUS Exhibit C*
- Information Security Policy – *ASUS Exhibit D*
- Blue Hill Data Services Certification and SOC Reports – *ASUS Exhibit E*
- Microsoft Office 365 Certification and SOC Reports – *ASUS Exhibit F*
- Cross Country Computing Corporation Certification and SOC Reports – *ASUS Exhibit G*

3.5 Internal Controls, Security and Technology

3.5.1 A. ASUS will use a secure transfer method to collect audit data.

- SFTP/FTPS (secure file transfer over TLS 1.2 or higher or secure file transfer over SSH).
- Secure Web Transfer using HTTPS with TLS 1.2 or higher.

B. ASUS will have data-at-rest encryption for transferred data.

- For cloud storage vendors, link their compliance information for data-at-rest encryption of blob/object storage. Office 365 always encrypts data-at-rest and in-transit. Customer data within Microsoft's enterprise cloud services is protected by several technologies and processes, including various forms of encryption. (Customer data in this document includes Exchange Online mailbox content, e-mail body, calendar entries, and the content of e-mail attachments, and if applicable, Skype for Business content), SharePoint Online site content and the files stored within sites, and files uploaded to OneDrive for Business or Skype for Business.) Microsoft uses multiple encryption methods, protocols, and ciphers across its products and services to help provide a secure path for customer data to travel through our cloud services, and to help protect the confidentiality of customer data that is stored within our cloud services. Microsoft uses some of the strongest, most secure encryption protocols available to provide barriers against unauthorized access to customer data. Proper key management is also an essential element of encryption best practices, and Microsoft works to ensure that all Microsoft-managed encryption keys are properly secured.

Customer data stored within Microsoft's enterprise cloud services is protected using one or more forms of encryption. (Validation of our crypto policy and its enforcement is independently verified by multiple third-party auditors, and reports of those audits are available on the Service Trust Portal).

Microsoft provides service-side technologies that encrypt customer data at rest and in transit. For example, for customer data at rest, Microsoft Azure uses BitLocker and DM-Crypt, and Microsoft 365 uses BitLocker, Azure Storage Service Encryption, Distributed Key Manager (DKM), and Microsoft 365 service encryption. For customer data in transit, Azure, Office 365, Microsoft Commercial Support, Microsoft Dynamics 365, Microsoft Power BI, and Visual Studio Team Services use industry-standard secure transport protocols, such as Internet Protocol Security (IPsec) and Transport Layer Security (TLS), between Microsoft datacenters and between user devices and Microsoft datacenters.

In addition to the baseline level of cryptographic security provided by Microsoft, our cloud services also include cryptography options that you can manage. For example, you can enable encryption for traffic between their Azure virtual machines (VMs) and their users. With Azure Virtual Networks, you can use the industry-standard IPsec protocol to encrypt traffic between your corporate VPN gateway and Azure. You can also encrypt traffic between the VMs on your virtual network. In addition, new Office 365 Message Encryption capabilities allow you to send encrypted mail to anyone. Following the Public Key Infrastructure Operational Security Standard, which is a component of the Microsoft Security Policy, Microsoft uses the cryptographic capabilities included in the Windows operating system for certificates and authentication mechanisms. These mechanisms include the use of cryptographic modules that meet the U.S. government's Federal Information Processing Standards (FIPS) 140-2 standard.

FIPS 140-2 is a standard designed specifically for validating product modules that implement cryptography rather than the products that use them. Cryptographic modules that are implemented within a service can be certified as meeting the requirements for hash strength, key management, and the like. The cryptographic modules and ciphers used to protect the confidentiality, integrity, or availability of data in Microsoft's cloud services meet the FIPS 140-2 standard.

Microsoft certifies the underlying cryptographic modules used in our cloud services with each new release of the Windows operating system:

- Azure and Azure U.S. Government
- Dynamics 365 and Dynamics 365 U.S. Government
- Office 365, Office 365 U.S. Government, and Office 365 U.S. Government Defense

Encryption of customer data at rest is provided by multiple service-side technologies, including BitLocker, DKM, Azure Storage Service Encryption, and service encryption in Exchange Online, Skype for Business, OneDrive for Business, and SharePoint Online. Office 365 service encryption includes an option to use customer-managed encryption keys that are stored in Azure Key Vault. This customer-managed key option, called Customer Key, is available for Exchange Online, SharePoint Online, Skype for Business, and OneDrive for Business.

For customer data in transit, all Office 365 servers negotiate secure sessions using TLS by default with client machines to secure customer data. For example, Office 365 will negotiate secure sessions to Skype for Business, Outlook, and Outlook on the web, mobile clients, and web browsers.

- For on-premises storage, provide information on the data-at-rest encryption technology implemented. While ASUS's Information Security Policy does not allow for company data to be housed locally, Audit Services requires all mobile device, PC and Laptop hard drives to be encrypted before access company data. Bitlocker is used to encrypt PC and Laptop hard drives and Microsoft Intune Company Portal is used to enforce encryption requirements for mobile devices.

C. ASUS will use a "least privileged" access model.

- Only auditors working on the audit will have access to the data.
- Administrative access or permission changes will be logged.

- Audit workpapers are housed in Office 365 SharePoint sites specific to each audit. Access to each site is granted only to the assigned auditor(s) and to Audit Services Audit Management. All access and/or permission changes are logged and administrative access is limited to Audit Services Senior Management.

3.5.2 ASUS will ensure that any data communications whether remote or internal, with the state or with an entity under audit, will be secured using a minimum of TLS v1.2. Any required cipher suites, protocols or encryption technology that has been publicly exploited (published CVE) will be immediately remediated upon discovery, including any aforementioned minimum-security requirements.

Audit Services Information Policy requires the use of secure data transmission sites for the delivery or receipt of data in all instances. Audit Services employs Sharepoint for secure transmission and/or receipt of data. Microsoft uses and enables the use of industry-standard encrypted transport protocols, such as Transport Layer Security (TLS) and Internet Protocol Security (IPsec). Audit Services will employ a secure site provided by the holder, holder advocate or state entity as long as the site employs industry standard security and encryption protocols.

3.5.3 ASUS will not require the usage of Java, Silverlight, Adobe Flash, Active X Controls or any additional third-party plugins from the state or any third-party entity under audit.

3.5.4 ASUS will export and return data to the state in a commonly used format at no additional cost to the state, upon request.

3.5.5 Within one month of a contract award pursuant to this solicitation, and annually thereafter, ASUS will provide American Institute of Certified Public Accountants (AICPA) SOC-1, Type 2; or SOC 2, Type 2; or ISO 27001:2013 Certification from an ANSI accredited certification body; or CSTAR Level 2 State RAMP Moderate Certification to the state with bridge letters to provide assurance that controls are operating during any intervening periods. The SOC-1, Type 2 report should cover all the requirements listed in AICPA's Statement of Standards for Attestation Engagements No. 18 (SSAE No. 18). If the requirements are not met

annually, the **STO** will not authorize audits and may cancel participation in existing multi-state audits.

Data Security

ASUS recognizes that successfully performing unclaimed property audits requires the adherence to highest level of data security standards. Our data security environment is summarized below, and our detailed Information Security Policy is set forth in ***ASUS Exhibits, Exhibit D – Information Security Policy***. **ASUS** has taken substantial efforts to ensure that its policies, procedures and practices meet strict industry standards. In addition to the controls established for our main computer system, **ASUS** utilizes Microsoft Office 365 for our personal computers. Our top priority is the security and protection of the data that comes into our possession.

Therefore, all of our laptops have Bitlocker security software installed to prevent access to any data if the machine is compromised.

Customer data is stored in Office 365 datacenters that are geographically distributed while taking regional data location considerations into account. Datacenters are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Datacenter access is restricted 24 hours a day by job function—with only customer application and services access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous video surveillance, and two-factor authentication. The datacenters are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

The use of anti-malware software is a principal mechanism for protection of our assets in Office 365 from malicious software. The software detects and prevents the introduction of computer viruses and worms into the service systems. It also quarantines infected systems and prevents further damage until remediation steps are taken. Anti-malware software provides both preventive and detective control over malicious software.

As an example of the effectiveness of our data policies, **ASUS** had virtually no down time when the City of New York closed due to the COVID-19. Our employees were able to continue working remotely and kept servicing our client States.

Security, compliance, and privacy in Office 365 has two equally important dimensions:

- The first dimension includes Microsoft-managed service-level capabilities that include technologies, operational procedures, and policies that are enabled by default.
- The second dimension includes customer-managed controls that enable you to customize your Office 365 environment based on the specific needs of your organization, while still maintaining security and compliance.

Microsoft is recognized as an industry leader in cloud security. At the service level, they use a defense-in-depth strategy that protects our data through multiple layers of security (physical, logical and data).

A defense-in-depth strategy ensures that security controls are present at various layers of the service and that, should any one area fail, there are compensating controls to maintain security at all times. The strategy also includes tactics to detect, prevent, and mitigate security breaches before they happen. This involves continuous improvements to service-level security features, including:

- Port scanning and remediation
- Perimeter vulnerability scanning
- Operating system security patching
- Network-level distributed denial-of-service (DDoS) detection and prevention
- Multi-factor authentication for service access

Physical Layer – Facility

Customer data is stored in Office 365 datacenters that are geographically distributed while taking regional data location considerations into account. Datacenters are built from the ground up to protect services and data from harm by natural disaster or unauthorized access. Datacenter access is restricted 24 hours a day by job function—with only customer application and services access given to essential personnel. Physical access control uses multiple authentication and security processes, including badges and smart cards, biometric scanners, on-premises security officers, continuous cyber surveillance, and two-factor authentication. The datacenters are monitored using motion sensors, video surveillance, and security breach alarms. In case of a natural disaster, security also includes automated fire prevention and extinguishing systems and seismically braced racks where necessary.

Physical Layer – Network

Perimeter protection is implemented through the use of controlled devices at the network edge and on points throughout the network. The overarching principle of our network security is to allow only connections and communications that are necessary to allow systems to operate, blocking all other ports, protocols and connections. Access Control Lists (ACLs) implemented in the form of tiered ACLs on routers, IPsec policies on hosts, firewall rules and host based firewall rules are implemented in the network with restrictions on network communication, protocols, and port numbers. Edge router security allows the ability to detect intrusions and signs of vulnerability at the network layer. Networks within the Office 365 datacenters are further segmented to provide physical separation of critical back-end servers and storage devices from the public-facing interfaces.

Logical Layer

The logical layer of security involves many controls and processes implemented to secure the host machines, applications running on those hosts and from administrators that may perform any work on those host machines and applications.

AUTOMATED OPERATIONS

Most of the operations performed on hosts and applications by administrators are automated so that human intervention is reduced to a minimum, reducing the possibility of an inconsistent configuration or a malicious activity. This automated approach extends to the deployment of systems within our datacenters.

ADMIN ACCESS TO DATA

Administrator access to Office 365 and our data is strictly controlled. Core tenets of this process are role based access and granting personnel least privilege access to the service that is necessary to perform specific operations. These tenets are followed whether the access is physical or logical.

Access control happens at various levels:

- Personnel level to ensure that there are appropriate background checks and strict account management so that only those essential to the task may perform the task

- Role based access control
- A Lockbox process which allows:
- Just-in-time accounts with high-entropy passwords
- Access for a limited amount of time
- Access to take specific actions based on the role
- The servers in the Office 365 service have a pre-determined set of processes that can be run using Applocker
- Auditing and review of all access

ANTI-MALWARE, PATCHING, AND CONFIGURATION MANAGEMENT

The use of anti-malware software is a principal mechanism for protection of our assets in Office 365 from malicious software. The software detects and prevents the introduction of computer viruses and worms into the service systems. It also quarantines infected systems and prevents further damage until remediation steps are taken. Anti-malware software provides both preventive and detective control over malicious software.

Advanced Threat Protection

Office 365 provides robust email protection against spam, viruses and malware with Exchange Online Protection (EOP).

Security Monitoring and Response

Many threats target software vulnerabilities, but others attack operational weaknesses, which is why Microsoft uses the Operational Security Assurance (OSA) framework. OSA supports continuous monitoring, helps to identify operational risks, provides operational security guidelines, and validates that those guidelines are followed. OSA helps make Microsoft cloud infrastructure more resilient to attack by decreasing the amount of time needed to protect, detect, and respond to security threats.

Highly Secure End-User Access

Office 365 customer data and services are secured at the datacenter, network, logical, storage, and transit levels. In addition, it is critical to be able to control access to data and how it may be used. In the Office 365 service, Azure Active Directory is used as the underlying identity platform. This enables your tenant with strong authentication options granular control over how IT professionals and users can access and use the service. Office 365 also allows integration with an on-premises Active Directory or other directory stores and identity systems such as Active Directory Federation Services (ADFS) or third-party secure token systems (STSs) to enable secure, token-based authentication to services.

Data Loss Prevention

Although malware and targeted attacks can cause data breaches, user error is actually a much greater source of data risk for most organizations. Exchange Online provides data loss prevention (DLP) technology that identifies, monitors, and protects sensitive data and helps users understand and manage data risk.

Additionally, as part of **ASUS's** internal controls to ensure compliance with the terms of our contracts and associated state and federal security measures to safeguard data, **ASUS** also has a contract with Blue Hill Data Services, Inc. (BHDS). Blue Hill is a wholly owned subsidiary of BPO Management Services, Inc. and is headquartered in Pearl River, New York, about 25 miles North of New York City in the Blue Hill Plaza. The Blue Hill Plaza campus is comprised of two buildings specifically designed and constructed to house data centers. BHDS is a Tier 2, SAS70 compliant data center focused on delivering flexible, customized solutions and customer service excellence to its clients worldwide. All **ASUS** systems are managed and monitored 24/7/365 by BHDS support staff using advanced monitoring tools and techniques. All files and program source data are backed up daily and copies of the data are stored off-site for the purpose of recovery within 24 hours. The results of the testing performed by an independent auditor were found to be satisfactory. The SOC Reports for Blue Hill Data Services, Inc. (BHDS) can be found under ***ASUS Exhibits, Exhibit E – Blue Hill Data Services SOC Reports.***

Please refer to **ASUS's** Cyber Incident Response Plan found under ***ASUS Exhibits, Exhibit H – Cyber Incident Response Plan.***

In addition, Microsoft Corporation SOC Reports can be found under ***ASUS Exhibits, Exhibit F – Microsoft Corporation SOC Reports*** and the Cross Country Computing Corporation Certification and SOC Reports can be found under ***ASUS Exhibits, Exhibit G – Cross Country Corporation Certification and SOC Reports.***

- 3.6 References:** As directed, **ASUS** offers the following three (3) States as references from governmental agencies which administer unclaimed property programs for which ASUS performed unclaimed property audits in the past five (5) years. As previously stated, **ASUS** currently has contractual arrangements with forty-four (44) states and the District of Columbia as identified in **ASUS Exhibit I – Contract States** and these states are offered as references as well.

State # 1

STATE OF LOUISIANA

Kathleen Lobell, Director
Louisiana Department of Treasury
Unclaimed Property Division
PO Box 91010
Baton Rouge, LA 70821
Phone: (225) 219-9377
Fax: (225) 219-9381
Email: klobell@treasury.state.la.us
Contract Term: 2001 to present

State # 2

STATE OF NEW JERSEY

Steven Harris, Administrator
New Jersey Treasury
Unclaimed Property Division
PO Box 214
Trenton, NJ 08625
Phone: (609) 777-4655
Fax: (609) 984-0593
Email: Steven.Harris@treas.nj.gov
Contract Term: 2003 to present

State # 3

STATE OF TEXAS

Matthew Angus, Audit Manager
Texas Comptroller of Public Accounts
Unclaimed Property Division
PO Box 12019
Austin, TX 78711
Phone: (512) 463-5225
Fax: (512) 463-3569
Email: Matthew.Angus@cpa.texas.gov
Contract Term: 2004 to present

3.7 Experience: ASUS has over twenty-five (25) years of experience in providing unclaimed property multi-state audit services for state governments. Most of our employees have over twenty (20) years of unclaimed property experience and are made up of many former state administrators, audit supervisors, attorneys, as well as private sector unclaimed property industry veterans. **ASUS** has the expertise, experience, skills and knowledge to identify and recover unclaimed property belonging to the citizens of the State of West Virginia. If awarded this contract, the resources expended by **ASUS** will be focused on serving as directed by the West Virginia Unclaimed Property Program.

As a contractor to the forty-four (44) states and the District of Columbia for whom we currently provide unclaimed property identification, collection and processing services we regularly exchange information with these states concerning issues of current concern to each of them. Additionally, **ASUS** presently supports the State of West Virginia as an authorized state service provider. As such, we are directly experienced in working with West Virginia and complying with its contractual and statutory requirements. We would expect, as a contractor to the State that we would maintain the same kind of interaction and exchange with the personnel of West Virginia's Unclaimed Property Program.

On average, **ASUS** completes over six hundred (600) audits per year, resulting in approximately \$50-75 million in unclaimed property reporting to the states and the District of Columbia. Since its inception, **ASUS** has remitted over \$1.2 billion to the respective state unclaimed property programs.

ASUS personnel have conducted audits that include, but are not limited to those in the following industries:

- Healthcare
- Rebates
- Insurance
- Airlines
- Brokerage
- Retail
- Fast food
- Financial Institutions
- Hotels
- Manufacturing
- Mutual Funds
- Service
- Utilities

3.8 Standards: ASUS will comply with the professional standards required by the American Institute of Certified Public Accountants (AICPA). The audit and identification of unclaimed property from the records of Holders, the processing of records and the demands for payment of the property to the STO will be made in accordance with the Act, Generally Accepted Accounting Principles (GAAP) and Generally Accepted Auditing Standards (GAAS) to the extent applicable to unclaimed property audits. ASUS will adhere to neutral, unbiased accounting and financial reporting standards based on the core value of independence as outlined by the Governmental Accounting Standards Board (GASB).

3.9 Staff Qualifications

3.9.1 Experienced Staff: All personnel assigned to audit engagements have the experience necessary to comply with this RFQ. ASUS is proud to affirm that most of our staff is comprised of a combination of former State employees who made their career in unclaimed property or individuals from the private sector who had worked primarily in the field of unclaimed property. ASUS is an affiliate of the **National Association of State Treasurers (NAST)** and is an active participant with the **National Association of Unclaimed Property Administrators (NAUPA)**. Also, Jeremy Katz, an ASUS partner, participates annually on NAUPA education panels, and has previously served NAUPA and NAST in the following capacities: Serving a second 3 year term on the National Association of State Treasurer's Corporate Affiliate's Board; Served two 2 year terms on National Association of State Treasurer's Foundation Board; Served as lead faculty advisor for National Institute of Public Finance Treasury Management Program and Served as an observer to the Uniform Law Commission with respect to the revision of the Uniform Unclaimed Property Law. In addition, we actively seek membership in other professional organizations which provide information that enables us to remain current on industry issues and state specific issues, such as the American Bar Association (ABA) and the National Conference of State Legislators (NCSL). In summary, those organizations include:

- The National Association of State Treasurers (NAST)
- The National Association of Unclaimed Property Administrators (NAUPA)
- The National Institute of Public Finance (NIPF)
- The Uniform Law Commission
- The American Bar Association (ABA)
- The National Conference of State Legislators (NCSL)

ASUS presents this background of experience to demonstrate that it is cognizant of the services required by the State because members of our staff were charged with the responsibility of securing similar contracts described in this RFQ in order for their state to ensure compliance with the unclaimed property laws. To this end, they also contracted with vendors who were capable of identifying and conducting compliance audits of selected holders of all categories of unclaimed property. In addition, we know and understand the sensitivities of the holders when conducting audits for unclaimed property. The experience gained by members of our staff while they worked for their State will serve as an asset to the West Virginia Office of the State Treasurer if again awarded a contract.

An organization chart that identifies the individuals who will be responsible for each of the required services outlined in the RFQ may be found in **ASUS *Exhibit A – Organizational Chart***. The staff members identified will support the requirements involving services such as holder research, auditing, information systems support, invoicing, etc. In addition, provided below is a summary of qualifications on the staff that will be available to provide services in response to this RFQ.

Matthew Thornton, Principal and Director of Operations. (A resume can be found under **ASUS *Exhibit J – Employee Resumes***). Mr. Thornton will oversee the entire operations of ASUS and coordinate the efforts of the staff to ensure maximum efficiency. He will oversee all issues dealing with data conversion, the generation of all state reports and invoices, quality management and improvement efforts and the management of Audit Services' trust accounts. In addition, Mr. Thornton is responsible for all systems development and testing projects and ensuring Audit Services' systems are in compliance with state reporting requirements.

Prior to joining Audit Services in 2004, Mr. Thornton was a Vice President at ACS-Unclaimed Property Recovery & Reporting where he was responsible for the due diligence and escheatment programs for both the MetLife and John Hancock Demutualizations. Under these programs more than \$2.5 Billion was either returned to owners or escheated to various states. He was also responsible for the Maximum Ownership Return program that targeted the return of property to high value shareholders for ACS-UPRR's corporate actions customers. Before UPPR, Mr. Thornton was a Vice President/Senior Project Manager at Mellon Investor Services where he had a leadership role in several multi-million dollar, high profile projects including: MetLife's Demutualization and IPO; the merger of NationsBank and BankAmerica; the relocation and reengineering of Investment Plan Services Department; the reengineering and expansion of Employee Products' Client Implementation Team; implementation of a strategic alliance with JPMorgan / American Century; and the transition of significant systems development effort from external to

internal support during the key rollout phase. Prior to Mellon Investor Services, Mr. Thornton was a Business Systems Consultant / Project Manager at American Management Systems, Inc. and Manager of Financial Planning, Analysis and Internal Consulting at First Chicago Trust Company of New York. Mr. Thornton holds a BBA in Finance from the University of Massachusetts at Amherst, an MBA from Fordham University's Graduate School of Business and has earned a Project Management Professional (PMP) Certification from The Project Management Institute.

Jeremy Katz, Partner. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). All state unclaimed property initiatives are led by Jeremy Katz, a nationally known unclaimed property professional with over twenty-seven (27) years of experience in unclaimed property. Jeremy joined Audit Services in December of 2016 and was previously with PRA Government Services (now called Avenue Insights). Prior to joining PRA-GS in September of 2014, Jeremy spent 20 years with Xerox (by way of several acquisitions including that of The National Abandoned Property Processing Corporation (NAPPCO) and Affiliated Computer Services (ACS) Unclaimed Property Clearinghouse).

While at Xerox, Jeremy was deeply involved in developing solutions and managing large teams of people responsible for the delivery of services to state unclaimed property programs. Specifically, Jeremy supported the implementation of complex database management systems, the creation of unclaimed property compliance and collections related solutions (one of which is patented by the U.S. Patent and Trademark Office), marketing and sales initiatives, contract management and strategic planning.

Jeremy has also developed and participated in training programs designed to educate state personnel on matter of unclaimed property and speaks frequently at national meetings on matter of unclaimed property compliance and owner reunification efforts. Other areas of focus have also included business process outsource and information technology-related solutions, including: finance and tax applications, cloud-based computing, infrastructure management, enterprise content management and application development and maintenance.

Jeremy actively participates as a Corporate Affiliate and former Corporate Affiliate Board member of the National Association of State Treasurers (NAST) and attends all NAST meetings and the meetings of the National Association of Unclaimed Property Administrators (NAUPA). Jeremy served two terms on the NAST Foundation Board and served as the lead faculty advisor for National Institute of Public Finance Treasury Management Program (unclaimed property). Lastly, Jeremy was an observer to the Uniform Law Commission as it undertakes the process of revising the 1995 Uniform

Unclaimed Property Act and frequently provides input to the states with respect to matters of legislation and litigation.

Jeremy is a graduate of the University of Maryland and has focused his continuing professional education in the areas of business and marketing management at Johns Hopkins University.

Benjamin “Benny” C. Spann, Chief Executive Officer. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Mr. Spann will be responsible for overseeing all facets of the contract and responding to any problems or questions that may arise. Duties will also include ensuring that approval is obtained from the State prior to the commencement of an audit, that monthly work-in-progress reports are provided in a timely manner, and release and indemnification agreements if necessary are prepared. In addition, in this capacity he will be tasked with assisting in the resolution of any conflicts that may occur during the course of an audit. Additional duties include responsibility for all state unclaimed property relationships involving contract renewals and negotiations and the resolution of issues involving the remittance of funds to client states.

Benny has over 25 years’ experience in the state administration of unclaimed property. He started his career as a corporate tax auditor with the Louisiana Department of Revenue. After a short while in the field, he moved into Field Services management. He then transferred into the unclaimed property world as Director of Unclaimed Property for the State of Louisiana responsible for the first total revision of the Louisiana unclaimed property statutes. The Unclaimed Property program was transferred to the State Treasurer’s office from the Department of Revenue in 2000. He continued to be the Director of this division until his retirement in June, 2012 after 36 ½ years of state service. He has been an active participant in the National Association of Unclaimed Property Administrators (NAUPA) serving as Southern Regional Vice President and serving on the uniform electronic reporting committee. He developed the NAUPA bulletin board system prior to the internet and also developed NAUPA’s first internet website. He has been awarded the NAUPA President’s award and the NAUPA Lifetime Achievement award. Benny started with Audit Services US LLC in September, 2013. He has an accounting degree from Louisiana Tech University in Ruston, Louisiana.

Amy Manganaro, Senior Auditor. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Amy is a senior unclaimed property auditor with more than ten years of experience in unclaimed property auditing. Prior to joining Audit Services, Amy was an Audit Supervisor with PRA Government Services and the Xerox Unclaimed Property

Clearinghouse. Amy's focus at PRA and Xerox was on general ledger unclaimed property audits of many of the nation's largest companies. Audits also included insurance companies as well as holders/processors of rebate checks.

Before joining Xerox, Amy was an Accounting Supervisor for AIM Healthcare, where one of her duties was to manage the process for unclaimed property compliance. In that role, she was active in the Unclaimed Property Professionals Organization (UPPO) and attended unclaimed property related conferences on a regular basis in order to network with other professionals in the unclaimed property arena as well as to keep apprised of changes in regulations and gain a better understanding of unclaimed property best practices.

Amy graduated from Eastern Nazarene College with a B.A. in Business Administration and from Trevecca Nazarene University with an MBA.

Erik Kallevik, Senior Auditor. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Erik is a senior unclaimed property audit manager with more than ten years of experience in unclaimed property auditing. Prior to joining Audit Services US, Erik was an Audit Manager with Kelmar Associates LLC and Xerox Unclaimed Property Clearinghouse. Erik's focus at Kelmar and Xerox was on general ledger unclaimed property audits of many of the nation's largest companies. Audits also included insurance, oil and gas and healthcare service companies. Before joining the unclaimed property industry, Erik was an accounting manager for Forrester Research Corporation and First Act, Inc., where one of the duties was to manage the process for unclaimed property compliance. Erik also has experience in working at the professional accounting firm, KPMG, conducting internal audits to assist clients in federal and state regulatory compliance. Erik graduated from University of Massachusetts at Amherst with a B.S. in Resource Economics and a concentration in Managerial Accounting.

James C. Dowley, Senior Auditor. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Jim has recently been hired by ASUS as a part-time auditor. Jim has over twenty-nine years experience in unclaimed property with the State of Ohio and Conduent State & Local Solutions, Inc. (formerly Xerox). Jim was previously an Unclaimed Funds Auditor 4 and then Compliance Supervisor with the Ohio Division of Unclaimed Funds. He then became the Director of Audits with Conduent State & Local Solutions, Inc. Jim graduated from The Ohio State University with a B.S. in Business Finance.

William Joseph, Reports and Processing Systems Manager. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Mr. Joseph will be responsible for the electronic reporting functions to the State, as well as performance monitoring and report

management. This requires that he check through NAUPA files and incoming audits and convert them to a format useable by the server prior to the submission of reports to our contract states. He is also responsible for the design and development of the work-in-progress reports remitted to the contract states. Mr. Joseph has experience in numerous software applications including Visual Basic, Visual FoxPro, Visual C++, HTML, Java, the entire Microsoft Office Suite, and COBOL. He has worked as the network administrator for Dunlop, Onderdonk and Wilson Corp., a small insurance agency that has since been sold and merged with Bollinger Inc. While working with Dunlop, Onderdonk and Wilson Corp., his duties included the day to day maintenance of the network, as well as training the employees how to use a Windows based PC software, and internet applications. He has created numerous professional websites for businesses, and he is currently developing a new and improved Work-in-Progress Report that is individualized for State Unclaimed Property Offices across the nation. He is currently working on his Bachelor's degree in Computer Science at William Paterson University with plans to obtain a Master's Degree in Computer Science as well.

Virgilio Capala, Jr., Escheatment Systems Analyst. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Mr. Capala is an Escheatment Systems Analyst with over 14 years of experience in the field of Unclaimed Property. Prior to joining Audit Services, Virgilio worked at Computershare, BNY Mellon Shareowner Services, Mellon Shareholder Services and Chasemellon Shareholder Services. Virgilio has a Diploma in Computer Programming from The Chubb Institute in Jersey City, New Jersey.

Jeffrey Saitta, Senior Programmer. (A resume can be found under *ASUS Exhibit J – Employee Resumes*). Mr. Saitta is responsible for maintaining Audit Services' proprietary system that allows us to file unclaimed property reports to our contract states. Mr. Saitta has over 25 years of programming experience in the field of Corporate Reorganization and Unclaimed Property. He was responsible for developing a complete Abandoned Property application providing data conversion functionality, due diligence and property eligibility testing and NAUPA file and state form/report generation. He is responsible for all ongoing maintenance and new development of the software used by Audit Services' staff.

David Potter (Legal Support). (A resume can be found under *ASUS Exhibit J – Employee Resumes*). David Potter is an accomplished litigator, having conducted over 35 jury trials, 100 bench trials and hearings, and numerous appellate arguments in state and federal courts. For over 25 years, he served as a faculty member for the National Institute of Trial Advocacy and Hofstra University Trial Techniques Program. Mr. Potter has also been a frequent commentator on Court TV.

Mr. Potter began his legal career as a New York City Assistant District Attorney, where he initially handled drug, larceny and corruption cases. Less than three years after joining the District Attorney's office, he was promoted to the position of trial attorney in the Homicide Bureau. Mr. Potter later joined a 60-lawyer business law firm in New York and transitioned into civil litigation.

In 1993, Mr. Potter co-founded the law firm of Lazare Potter & Giacobas (now Lazare Potter Giacobas & Moyle), where he continued representing clients in a wide range of commercial matters. He currently represents clients in complex commercial litigations, arbitrations and mediations, contract negotiations and employment matters.

Education

- Albany Law School of Union University, Albany, New York (J.D., 1986 - Recipient, Order of the Barristers Award)
- St. Lawrence University, Canton, New York (B.A., 1982)

Bar Admissions

- States of New York and Massachusetts • District of Columbia
- U.S. Court of Appeals for the Second Circuit
- U.S. District Courts for the Southern and Eastern Districts of New York

3.9.2 Partner & Supervisory Qualifications: All **ASUS** personnel will serve as the project team. Their qualifications and experience have been described in subsection 3.9.1.

All current state unclaimed property auditing initiatives are led by Jeremy Katz, a nationally known unclaimed property professional with over 25 years of experience working on behalf of all of the states. Jeremy's detailed unclaimed property experience are set forth below along the qualifications and experience of the unclaimed property team available for assignment to manage the present contract and perform the ongoing holder examination reporting, and collections tasks to be performed under the RFQ.

A company organizational chart (which can be found under ***ASUS Exhibits – Exhibit A – Organizational Chart***) illustrates the team assigned to the identification, examination and collection of unclaimed property from holders on behalf of **ASUS** State clients. The activities, hours allocated, and costs associated with the operation of the audit organization are coordinated in several weekly staff meetings, as well as by using electronic cloud-based contact, recordkeeping and management tools.

All operations, custody and reporting matters are managed out of our New York City based headquarters and are led by Matthew Thornton. Matthew's detailed experience is set forth above. Matters relating to audits, contract compliance or other matters relating to supporting West Virginia may be addressed to Jeremy, Matthew or Benjamin Spann (whose biography is also set forth below). Lastly, **ASUS** believes in working closely with its client's states and is routinely in directly contact via email, phone and in person meetings as requested.

3.9.3 Continuation of Quality Staff: As previously stated, **ASUS** is now in its twenty-fifth year as a contract vendor to provide auditing services to the states we serve. All **ASUS** personnel have five (5) or more years of experience in performing unclaimed property audits, and **ASUS** affirms that any staff replacements will have the same or greater qualifications, training and experience as the staff member they may replace. **ASUS** agrees to notify the **STO** of any personnel or staff changes that would affect the services provided to the **STO**.

3.9.4 Subcontractors: **ASUS** does not use or intend to use any subcontractors in performance of any work contemplated by this RFQ.

4.1 Mandatory Contract Services Requirements and Deliverables:

4.1.1 Specific Work Plan – Audits: ASUS agrees with the requirements of this section and will comply accordingly. ASUS will adhere to the audit guidelines set forth in the ASUS Audit Program and the ASUS Audit Operating Procedures Manual – see **ASUS Exhibits B and C** respectively.

4.1.2 Audit Examinations: ASUS agrees with the requirements of this section and will comply accordingly. Specifically:

ASUS Audit Programs

Recognizing that each state and the District of Columbia may approach unclaimed property auditing slightly differently, ASUS has developed three customizable variations of its unclaimed property auditing program to support the identification and collection of unclaimed property. In each case, the State can elect to participate and authorize audits under any or all of the different programs. The ASUS unclaimed property auditing programs include:

- Comprehensive General Ledger Audits
- Securities Compliance Audits
- Contractor Assisted Self Audits (CASA) – *Referred to as “Vendor Assisted Self Audits” in the RFQ*

At the time of its authorization request, ASUS will indicate the type of audit proposed in accordance with the RFQ Pricing Page – (i.e. – multi-state audit, voluntary compliance, agreed upon procedures or vendor assisted).

The ASUS programs are described in detail below.

A detailed audit manual/procedure is set forth in **ASUS Exhibits, Exhibit C – Audit Operating Procedures Manual**. In summary, upon authorization from the State, ASUS will:

- contact persons, firms, and entities (“holders”) that are in possession of such property,
- audit such holders to determine the value of property held and due to the State,
- report to the State the results of audits in progress and completed
- facilitate the transfer to the State unclaimed property from audited holders and/or their agents, and

- perform other related duties, as required by the State's documented procedures, and in accordance with and all federal legislation rulings regarding unclaimed property.

In most cases, a Non-Disclosure Agreement (NDA) is executed between **ASUS** and the holder, and an opening conference is scheduled.

The examination of the books and records of holders of unclaimed property and the demand for delivery of such property is made pursuant to the following principles:

- 1.) The requirements as outlined by the State, including the requirements specified in the State's unclaimed property law.
- 2.) The holdings of the U.S. Supreme Court in *Texas v. New Jersey*, 85 S. Ct. 626 (1965); *Pennsylvania v. New York*, 92 S. Ct. 2075 (1972); and *Delaware v. New York*, 113 S. Ct. (1150 1993), regarding which state has the right to escheat property, is followed, specifically:
 - Where the name and last known address of the apparent owner according to the books and records of the holder is in a particular state, it will be deemed reportable to that state.
 - If the holder has no records identifying the name and last known address of the apparent owner, the property will be deemed reportable to the state of incorporation of the holder.
- 3.) An address will be deemed to mean a description of location sufficient for the delivery and/or receipt of mail or is otherwise sufficient to identify the apparent owner and the state wherein the apparent owner resides or resided.
- 4.) Where the holder's books and records reflect that the holder did maintain the names and addresses of apparent owners, but such records are no longer retained or are not readily available, sampling and other examination techniques may be utilized to determine the total amount of reportable property when permitted by individual state law.
- 5.) **ASUS** will obtain the assurance from the holder that it has complied with the due diligence requirements of the statutes with respect to finding the owner of property prior to remitting it to the State.
- 6.) **ASUS** will instruct the holders to file future reports with the State pursuant to the State's reporting requirements.

7.) Property will be transferred in trust for the State to the custodian or remitted directly by the holder.

Our examinations of Holders for Unclaimed Property include the following processes:

- Research of audit leads for approval submission
- Strict approval process with client states
- Thorough analysis of internal controls
- Review of the Chart of accounts for determining property types involved
- Review of the holder's organizational structure (i.e., parent company, subsidiary, etc.)
- Review of policy and procedures manual that identifies the handling or disposition of unclaimed accounts
- Interviews with Holder staff over each functional control of property types
- Sampling records for exceptions as appropriate and permitted
- Constant and open communications with Holder representatives or employees
- Investigation of available address data to determine owner location and dormancy
- Case law knowledge for application to each examination
- Report writing including findings summary by state, by period and by property type
- Quality review process handled at supervisor, and again at upper-management level
- Discussion of audit findings with Holder and the State

ASUS also recognizes the need to complete unclaimed property examinations in a timely and efficient manner, and our auditors are trained to adhere to our audit procedures to ensure this occurs. It is our policy to open and engage in no more examinations than we feel we have capacity to properly handle, and the examination should be commenced no more than ninety (90) days from the date the holder is notified of our intent to perform the examination. In the event there is a scheduling conflict or problems with providing records, **ASUS** will work with the holder to resolve these issues. In any case, the State will also be notified of any changes.

AUDIT PROPOSAL AND AUTHORIZATION – Vendor-Proposed and Division-Proposed Audits – (Identifying Candidates for Audit)

Our process for conducting an unclaimed property examination begins with a thorough research of the holder's reporting history. To identify holders, we look for companies

doing business in particular industries -- such as insurance, retail, utilities, banking, etc. -- where instances of unclaimed property typically occur. Companies in these categories that are flagged for further review include those that:

- do not report unclaimed property,
- submit reports indicating no unclaimed property to report,
- omit types of property typically found within the company's industry,
- or report amounts significantly at variance with industry norms.

Other considerations are companies involved in recent mergers or acquisitions, and companies in industries that typically employ a large transient workforce. In some cases we may also be asked by a state to audit specific holders already known to the state.

Pre-audit research may also include: assessing companies for annual revenue, number of employees, state of incorporation, overall market share and industry practices. Once information is gathered, the companies are typically compared to filing data supplied by various states. Once apparent non-compliance companies are identified, **ASUS** may send audit authorization requests to the State or one or more other states for approval. Typically, **ASUS** will solicit multiple, if not all states to join a general ledger audit. States will then have the opportunity to either initiate or join an audit that has already been initiated by one or more other states.

While audit recommendation criteria are defined in close consultation with our clients, our general guidelines may also include reviewing the following information:

- SIC Codes – is type or size of business of the audit candidate likely to give rise to unclaimed property?
- Annual Revenue - is the business large enough to generate material amounts of unclaimed property, sufficient to warrant the cost of an audit?
- Age of Business - has the business been in operation long enough to have property that has reached its dormancy period?
- Reporting History – is there evidence that would lead an objective reviewer to conclude that reporting has been complete and consistent?

Research data is gathered from publicly available sources such as: EDGAR filings, Dun & Bradstreet, Standard and Poor's and A.M. Best's.

ASUS acknowledges that the State reserves the right to participate in or restrict its participation in an audit of any holder. Prior to beginning any audit, **ASUS** will draft and submit to the State an engagement letter (Sample **Authorization/Engagement Letter** attached set forth in ***ASUS Exhibit K – Sample Audit Authorization/Engagement Letter***) which defines agreed upon procedures, at a minimum:

- All holders, including all subsidiaries or affiliated holders, included in the scope of the audit, identified by both FEIN and Legal Name;
- Time period of records to be examined;
- Specific scope of types of records and/or transactions to be audited;
- Audit selection criteria used;
- Frequency and/or timing of reporting identified unclaimed property during an audit;
- Anticipated begin date of audit; and
- Anticipated time to complete audit;

ASUS acknowledges that it will not begin any audits pursuant to the contract until after the engagement letter, with agreed upon procedures, has been accepted and signed by the State.

- In conjunction with the identification and collection of property, the ASUS agrees that it shall:
- Request audit authorizations in accordance with the requirements as set forth by the RFQ;
- Audit the records of holders or potential holders to identify with specificity the unclaimed property that should be reported and delivered to the State;
- Advise holders that all property reported and remitted must conform to The State reporting requirements;
- Prepare and submit to the State reports of property in accordance with the requirements of the statute and as stated in the agreed upon procedures;
- Request holders and their agents to deliver to the Vendor, or the Vendor's custodian, property deemed owing in accordance with the RFQ requirements
- Forward the property to the State or its designee.

PERFORMANCE OF AUDIT

Audit Uniformity

To ensure uniformity in our audits, we utilize our Audit Operating Procedures Manual mentioned above, which is used by our auditors in the review and audit process to determine and accurately report the holder's unclaimed property liability. This Manual is an essential tool utilized in the conduct of our work. Areas discussed in the Manual include, but are not limited to ascertaining the availability of records, requesting records, evaluating records, identifying property, categorizing property identified, evaluating potential and actual findings, and collecting and remitting property found. In addition, we cover in our procedures issues dealing with cooperating with other contract vendors when auditing the same holder, professional conduct, training unclaimed property auditors, utilizing estimation techniques, and how to deal with problem holders. Other important issues include actions to be taken if there is an audit protest, and the filing and maintenance of audit files that must be retained for possible review by the State and our contract states.

In addition to this industry standard, **ASUS** maintains its own strict procedures, and we closely follow our Audit Program in the conduct of our examinations. The Audit Program provides a checklist to ensure that all facets of the audit are covered, while the Audit Operating Procedures Manual dictates the methodology for conducting the audit.

General Ledger Audit Program

As authorized by the State, **ASUS** can schedule and complete unclaimed property audits, where there may be reason to believe that the holder has never reported or reports submitted by such holders are incomplete or appear to have errors. In summary, upon authorization from the State, **ASUS** will:

- contact persons, firms, and entities ("holders") that are in possession of such property,
- audit such holders to determine the value of property held and due to the State,
- report to the State the results of audits in progress and completed
- facilitate the transfer to the State unclaimed property from audited holders and/or their agents, and

- perform other related duties, as required by the State's documented procedures, and in accordance with and all federal legislation rulings regarding the Uniform Unclaimed Property Act.

Typically, **ASUS** will solicit multiple, if not all of our client States to join a general ledger audit. The States will then have the opportunity to either initiate or join an audit that has already been initiated by one or more other states. In most cases, an NDA is executed between **ASUS** and the holder, and an opening conference is scheduled.

The identification of unclaimed property is facilitated by performing an analysis on a number of items, including but not limited to: (1) the holder's chart of accounts (each different type of entity has a different chart of accounts); (2) the holder's organizational structure (i.e., parent company, subsidiary, etc.); and (3) any policy and procedures manual that identifies the handling or disposition of unclaimed accounts. In the course of an audit of a holder's records, a demand will be made for any property that has been identified as unclaimed, provided it comes under the purview of the State's Unclaimed Property Law.

This of course will require a careful analysis of the custodial periods required by each State under its own law. To this end, **ASUS** has developed its own matrix on the custodial periods for each State. Once property has been identified as unclaimed and demandable, it will then be forwarded to the State or the State's designee on the form or magnetic media specified by the State.

ASUS also recognizes the need to complete unclaimed property examinations in a timely and efficient manner, and our auditors are trained to adhere to our audit procedures to ensure this occurs. It is our policy to open and engage in no more examinations than we feel we can handle within a prescribed time frame, and the examination should be commenced no more than 90 days from the date the holder is notified of our intent to perform the examination. In the event there is a scheduling conflict or problems with providing records, **ASUS** will work with the holder to resolve these issues. In any case, the State will also be notified of any changes.

Once approval has been obtained from the State, a letter is sent to the holder notifying them of the audit and providing basic information regarding the audit process. The letter also serves to educate the holder about **ASUS'** role and appropriate references to the State law and their obligations under the law.

Contact is established by **ASUS** with the holder and mutually agreeable date is set to hold an Opening Conference and begin a review of records. A letter is sent to confirm this time, respond to any initial questions, and to request initial records needed for the review. The Opening Conference provides the auditor time to explain the scope, establish a timeframe

and begin the review of the items initially requested. The holder has the opportunity to ask questions and voice concerns as well as discuss the audit process in general.

Because **ASUS** serves the State, the State will be notified immediately if the holder should become uncooperative and unwilling to comply with the requirements of the examination. In situations where holders are uncooperative in the examination, it is possible for the examination to extend for more than one year. This usually occurs in accounting and/or auditing methodology or in the interpretation of the law. Also, in the event the holder has numerous divisions that must be examined, the audit process could be lengthy, but the State will be kept well informed of the progress and we will seek direction and assistance from the State if a problem should occur.

Once fieldwork begins, our auditors meet with the company in an entrance conference, performed in person and/or by teleconference. This interview is held with the appropriate company personnel to access internal controls and procedures concerning unclaimed property identification and reporting. We also review the holders organizational structure to determine areas of possible liability by property type and perform proper analysis depending upon property type.

The fieldwork involves a review of the holder's chart of accounts and internal controls, a detailed review of accounting records and a test of transactions is performed to identify various types of unclaimed property. In the event that some records are unavailable, estimates, in accordance with accepted State practices, are developed.

Some audits require additional procedural efforts, related to the statute of limitations within the law. This is either due to missing records, refused records or concerted efforts by companies to disregard any legally required commitment for filings, record retention and adequate staff training.

Inadequate records are approached in several ways, depending on what data is available. Investigative steps are used during our analysis of internal controls to discover trends overall and the source and volume of errors either in units or dollars. Once a well-documented basis for extrapolation is determined, we are able to project liability.

Upon completion of the fieldwork, an extensive review is performed by our Audit Division management to ensure all potential property types have been addressed, and holder issues resolved in a professional manner. If a holder fails or refuses to report or deliver unclaimed property within fifteen (15) days of notification **ASUS** will notify the State in writing prior to initiating any further action.

Holder Due Diligence and Subsequent Reporting

ASUS will obtain the assurance from the holder that it has complied with the due diligence requirements of the statutes with respect to finding the owner of property prior to remitting it to the State.

ASUS will instruct the holders to file future reports with the State pursuant to the State's reporting requirements

Unclaimed Property Report

It is ASUS's policy to file an unclaimed property report and invoice with the remittance when an examination is completed. All raw data obtained from the examination is input (physical or download) into our own proprietary software (*ASUS Exhibit L – Audit Services System*).

The *Audit Services System* is compliant with all 50 states' requirements and utilizes the NAUPA II standard reporting format, among others for reporting unclaimed property to client states. We recognize that providing accurate and precise information that can be downloaded to our client state's database is essential to the processing of data received in a timely and efficient manner. This information is necessary for not only accounting purposes, but to facilitate the possibility of the State locating the rightful owner.

ASUS will provide reports of the property to be forwarded to the State in a format prescribed by the State pursuant to the Uniform Disposition of Unclaimed Property Act, section 36-8-1 et seq. of the **West Virginia** General Statutes.

Reports will include the following information:

- a. holder name
- b. holder address
- c. a holder contact, familiar with the records processed and the property transferred;
- d. Federal Employer Identification number of the holder;
- e. Owners' names;
- f. Owners' last known addresses;
- g. Owners' social security numbers or Federal Tax Identification numbers;
- h. Types of property;
- i. Any unique property identifier or number used by the holder;
- j. Amount of the property;
- k. CUSIP number and certificate numbers for any securities, if applicable;
- l. Bond numbers and coupon numbers accompanied with call date, if applicable;
- m. Value of the shares and the valuation date;
- n. Description of any securities, including maturity date, interest rates, and interest or dividends due, if applicable; and
- o. Date of the last transaction with the owner with respect to the property.

Delivery of Unclaimed Property

All unclaimed property received by **ASUS** or the Custodian shall be delivered to the Department within thirty (30) calendar days of Reconciliation or within one hundred twenty (120) calendar days of receipt, whichever occurs first or in accordance with requirements set forth by the Department. **ASUS** will determine the value of securities, at the closing bid price of any security trading on an exchange, on the date the security is transferred into the name of the State. If the security is traded in the over-the-counter market, then the security will be valued at the bid price as set forth in the pink sheets on the date the security is received by the State. In the event that the pink sheets do not contain the bid price for the security or the share(s), then **ASUS** will make recommendation to the State as to an alternate valuation technique.

All securities will be valued in accordance with generally accepted valuation procedures, subject to verification by the State. **ASUS** will submit verifiable documentation to the State regarding the date of the transfer of the securities, along with information indicating **ASUS's** proposed valuation of such securities transferred.

ASUS acknowledges that a complete delivery of property shall consist of the following:

- An unclaimed property report (NAUPA report, submitted online)
- A confirmation of each securities transaction
- A summary of all stocks or mutual funds delivered

Procedures Specific to Life Insurance Company Audits

As some of the audits performed by **ASUS** (Life Insurance and Retirement Account Property) require the ability to access and perform matching against the Social Security Administration Death Master File (DMF), **ASUS** retained the services of a leading DMF matching service provider - Cross Country Computer Corporation (“CCCC”). CCCC meets the highest standards for accuracy and date security. For your reference, a copy of their Information Security Management System certification is attached as ***ASUS Exhibit G – Cross Country Computer Corporation Certification and SOC Report***.

ASUS has fully tested the CCCC matching and reporting output, and has determined that the algorithms and results are consistent with the requirements of the insurer global resolution agreements, with the additional benefit of being scalable and having greater resolution between confidence levels to allow superior differentiation between strong,

weak and false-positive matches. Further, in our experience CCCC has maintained 100% system up-time while providing immediate access to subject matter experts as needed.

DATA MATCHING PROCESS

As authorized by the STATE, ASUS is able to provide data matching against the Social Security Death Master Index (DMF). ASUS has conducted audits of some of the nation's largest insurance and financial services companies that have involved secure DMF matching. Our service provider for this requirement is called Cross Country Computer Corporation ("CCCC"). CCCC is based in East Islip, New York and has been providing these services for over 10 years. They are ISO 27001:2103 standards and is SOC 1 Type 2 certified annually. CCCC meets the highest standards for accuracy and data security. For your reference, a copy of their Information Security Management System certification can be found under ***ASUS Exhibit G – Cross Country Computer Corporation Certification and SOC Report.***

Cross Country Computer uses its patented Abandoned Property Escheat Assignment & Reporting System (APEARS®) which satisfies state and audit mandates requiring fuzzy matching to the Social Security Administration's Death Master File (SSA DMF) to identify those who are deceased. APEARS® has been successfully utilized in support of all major insurance company demutualizations in recent history and with accuracy well in excess of 99%, has the ability to exceed the requirements set forth in all of the publicly available Global Resolution Agreements (GRAs) and Regulatory Settlement Agreements (RSAs), as well as all of the state-specific legislation including NY's Reg-200. The APEARS search functionality description for individual searches is set forth in ***ASUS Exhibit M – APEARS Instructions.***

ASUS has fully tested the CCCC matching and reporting output and has determined that the algorithms and results are consistent with the requirements of the insurer global resolution agreements, with the additional benefit of being scalable and having greater resolution between confidence levels to allow superior differentiation between strong, weak and false-positive matches. Further, in our experience CCCC has maintained 100% system up-time while providing immediate access to subject matter experts as needed.

Thomas Berger is our main point of contact. His brief bio follows:

Thomas Berger is Principal/President & Chief Executive Officer of **Cross Country Computer (CCC)**. Tom joined CCC in 1991 and acquired the company in 1996. During his tenure, Tom has overseen the debt-free growth of CCC and has been instrumental in strengthening the company's

infrastructure while simultaneously developing new services and diversifying into new business lines.

Tom has personally developed the vision and design specifications for many of CCC's systems, including TBeaut and CBeaut, our proprietary title and company name standardization products. In addition, Tom holds the patent for our **Abandoned Property Escheat Assignment & Reporting System (APEARS™)**.

Tom has served two terms as Treasurer of the Unclaimed Property Professionals Organization (UPPO) as well as two years as Secretary of the Unclaimed Property Committee within the Securities Transfer Association. He assisted in the creation of a white paper designed to educate the holder community about unclaimed property review and reporting practices. Tom has spoken frequently at Unclaimed Property conferences and was honored with the 2005 Unclaimed Property Holders Liaison Council's (UPHLC) President's Award.

Tom is also an active member in numerous direct marketing related organizations including the Direct Marketing Association of Long Island, where, in 2012, he was selected as one of three inductees into the DMALI Hall of Fame. He is also a lifetime member of MENSA, the international High IQ society. Tom holds a BS degree in Management and Marketing from the Rochester Institute of Technology and has received military security clearance to oversee our government accounts.

Global Resolution Agreements/Audit Resolution Agreements

From time to time, complex audit may require the use of complex agreements that set forth the agreed upon parameters of an unclaimed property examination. These agreements generally come at the request of the company being audited, and are typically executed by the participating state, the company under audit and the audit firm. ASUS has significant experience with these agreements and has worked with the states on many occasions where these agreements have been required. A sample agreement is set forth in ***ASUS Exhibit N – Sample Global Resolution Agreement***.

RULES FOR IDENTIFYING DEATH MATCHES

In comparing COMPANY's records of its insureds, annuitants, and Annuity Contract owners against the DMF, the governing principle to be followed shall be establishing whether or not a unique biological individual identified on COMPANY's data is the same as a unique biological individual identified on the DMF in a case where a benefit is due and payable. In comparing COMPANY's records of its insureds, annuitants, and Annuity Contract owners against the DMF, ASUS will divide the matches it identifies into three categories in accordance with the rules set forth below.

Category 1: SSN Match

A Category 1 Match occurs in any of the following circumstances:

1. There is a four-way exact match of the First Name, Last Name, Date of Birth, and Social Security Number contained in the data produced by COMPANY against data contained in the DMF;
2. The First Name matches in accordance with the Fuzzy Match Criteria listed below and the Last Name, Date of Birth, and Social Security Number match exactly.

Category 2: SSN Match

A Category 2 Match occurs when:

1. There is a four-way match of the First Name, Last Name, Date of Birth, and Social Security Number such that the Social Security Number contained in the data produced by COMPANY matches exactly to the Social Security Number contained in the DMF, and the First Name, Last Name, and Date of Birth match either exactly or in accordance with the Fuzzy Match Criteria listed below.

Category 3: Non-SSN Match

A Category 3 Match occurs in any of the following circumstances:

1. The Social Security Number contained in the data produced by COMPANY matches in accordance with the Fuzzy Match Criteria listed below to the Social Security Number contained in the DMF, and the First and Last Names, and Date of Birth match either exactly or in accordance with the Fuzzy Match Criteria listed below.

2. The records produced by COMPANY do not include a Social Security Number or where the Social Security Number is incomplete (less than 7 digits) or otherwise invalid (i.e. 000000000, 999999999, 000006789), and there is a First Name, Last Name, and Date of Birth combination in the data produced by COMPANY that is a match against the data contained in the DMF where the First and Last Names match either exactly or in accordance with the Fuzzy Match Criteria listed below and the Date of Birth matches exactly, subject to paragraph 3 immediately below.
3. If there is more than one potentially matched individual returned as a result of the process described in paragraph 2 above, then ASUS shall run the Social Security Numbers obtained from the DMF for the potential matched individuals against Accurant for Insurance or an equivalent database. If a search of those databases shows that the Social Security Number is listed at the address provided by COMPANY for the insured, then a Category 2 Match will be considered to have been made.

Fuzzy Match Criteria:

1. A First Name fuzzy match includes one or more of the following:
 - a. "First Name" "Nick Names:" "JIM" and "JAMES." ASUS utilizes the pdNickname database from Peacock Data, Inc. as well as publicly available lists of names and nicknames to identify matching First Names where a nickname is used on one or both sides of the match.
 - b. "Initial" instead of full first name: "J FOX" and "JAMES FOX"
 - c. "Metaphone" (a recognized and accepted phonetic name matching algorithm created by Lawrence Philips and originally published in 1990): "BUDDY" and "BUDDIE."
 - d. Data entry mistakes with a maximum difference of one character with at least five characters in length: "HARRIETTA" and "HARRIETA."
 - e. If First Name is provided together with Last Name in a "Full Name" format and "First Name" and "Last Name" cannot be reliably distinguished from one another: "ROBERT JOSEPH," Both "JOSEPH ROBERT" and "ROBERT JOSEPH."
 - f. Use of interchanged "First Name" and "Middle Name:" "ALBERT E GILBERT" and "EARL A GILBERT."
 - g. Compound "First Name:" "SARAH JANE" and "SARAH," or "MARY ANN" and "MARY."
 - h. Use of "MRS." + "HUSBAND'S First Name + Last Name:" "MRS DAVID KOOPER" and "BERTHA KOOPER" where the "Date of Birth"

and “Social Security Number” match exactly and the Last Name matches exactly or in accordance with the Fuzzy Match Criteria listed herein.

2. A “Last Name” fuzzy match includes one or more of the following:
 - a. “Anglicized” forms of last names: “MACDONALD” and “MCDONALD.”
 - b. Compound last name: “SMITH” and “SMITH-JONES.”
 - c. Blank spaces in last name: “VON HAUSEN” and “VONHAUSEN.”
 - d. “Metaphone” (a recognized and accepted phonetic name matching algorithm created by Lawrence Philips and originally published in 1990): “GONZALEZ” and “GONZALES.”
 - e. If First Name is provided together with Last Name in a “Full Name” format and “First Name” and “Last Name” cannot be reliably distinguished from one another: “ROBERT JOSEPH,” Both “JOSEPH ROBERT” and “ROBERT.
 - f. Use of apostrophe or other punctuation characters in “Last Name:” “O’NEAL” and “ONEAL.”
 - g. Data entry mistakes with a maximum difference of one character for Last Name: “MACHIARELLI” and “MACHIAVELI.”
 - h. Last Name Cut-off: A match will be considered to have been made where due to the length of the Last Name, some of the last letters were not saved in the database. Examples include: “Brezzinnows” and “Brezzinowski” and “Tohightower” and “Tohightowers.”
 - i. Married Female “Last Name” Variations: A fuzzy “Last Name” match will be considered to have been made even though the data does not match on the Last Name of a female, if the “Date of Birth” and “Social Security Number” matches exactly and the First Name matches exactly or in accordance with the Fuzzy Match Criteria listed herein.
3. A “Date Of Birth” fuzzy match includes one of the following:
 - a. Two dates with a maximum of one digit in difference: “03/27/1945” and “03/27/1946”
 - i. NOTE: “03/27/1949” and “03/27/1950” are not a match under Rule 3(a)i.
 - ii.
 - ii. Only 1 entry mistake per full date is allowable: “03/27/1945” and “03/28/1946” are not a match.
 - b. Transposition of “Month” and “Date” portion of the “Date of Birth:” “05/11/1935” and “11/05/1935.”
 - c. If either COMPANY’s systems or the DMF does not contain a complete “Date of Birth,” then a “Date of Birth” exact match will be found to exist where the data that is available on COMPANY’s systems does not conflict

with the data contained in the DMF. By way of example, if COMPANY's systems only contain a month and year of birth, an exact "Date of Birth" match will exist if the DMF record contains the same month and year of birth.

- d. If the COMPANY provided First and Last Name match, either exactly or in accordance with the Fuzzy Match Criteria listed herein, and the COMPANY provided Social Security Number matches exactly against the DMF, then the Date of Birth will be a fuzzy match if the COMPANY provided Date of Birth is within 2 years (either before or after) the DMF listed Date of Birth.
 - e. For all industrial policies (known internally at COMPANY was "intermediate and weekly policies" or "IWPs"), if the COMPANY provided First and Last Name match exactly and there is an inaccurate, missing or incomplete SSN, a match will be considered made if:
 - i. The COMPANY supplied Date of Birth is a default Date of Birth (e.g., 1/1/1915) and the DMF year of birth is either an exact match or DMF Date of Birth is within one year either before or after the insurer provided Date of Birth. [Examples: 1/1/1915 & 2/25/1915 or 1/1/1915 & 2/25/1916]
 - ii. The COMPANY supplied Date of Birth matches exactly with the DMF month and day of birth and the DMF year of birth are within five years before to five years after the insurer supplied Date of Birth. [Examples: 2/25/1915 & 2/25/1913 or 2/25/1915 & 2/25/1916]
 - iii. The COMPANY supplied Date of Birth matches exactly with the DMF month and year and the DMF day of birth is not a match. [Examples: 2/25/1915 & 2/15/1915 or 2/25/1915 & 2/7/1915]
 - iv. The DMF Date of Birth is within 5 years +/- of the COMPANY supplied Date of Birth and a search of that individual's First and Last Name and Social Security Number (listed on the DMF) in Accurant for Insurance or an equivalent database, results in an address matching a COMPANY address for that Contract.
4. A "Social Security Number" fuzzy match includes one of the following:
- a. Two Social Security Numbers with a maximum of two digits in difference, any number position: "123456789" and "123466781."
 - b. Two consecutive numbers are transposed: "123456789" and "123457689."
 - c. If a Social Security Number is less than nine digits in length (with a minimum of seven digits) and is entirely embedded within the other Social Security Number: "1234567" and "0123456789."

Description of Securities Procedures

Securities Audit Program

Securities compliance is a complex and burdensome task for both holders and the State. Audit Services' proprietary systems and audit methodologies help identify and correct recordkeeping errors, improper application of statutory requirements and unreported issues. Our highly specialized knowledge, combined with our proven technology, is then used to support the accurate and timely transmission of securities related owner information in a format that can readily be loaded into State systems, as well as facilitate the transfer of the securities to the State's designated custodian bank.

Most of these audits are on publicly traded corporations where it is necessary to request and review accounting records from their transfer agents or brokerage houses to complete the audit on the equity and debt side of the corporation. Proper analysis of equity property requires review of shareholder ledgers, undeliverable or unexchanged stock certificates arising from mergers and acquisitions, redemption payments, liquidations, dividend reinvestment plans, mutual funds, uncashed dividends, cash in lieu of fractional shares, stock splits, bank statements, outstanding dividends, retirement accounts and check listings.

For debt property we review records of matured or called debt (Bonds, Debentures, and Notes), unnegotiated interest checks, bank statements and reconciliations, unredeemed principal from calls of serial maturities, and unredeemed coupons from matured bearer issues.

Summary of Contractor-Assisted Self-Audits

Contractor-Assisted Self-Audit Program (CASA)

ASUS believes that compliance with the State's unclaimed property laws can be greatly increased by augmenting current State resources with our optional Contractor Assisted Self Audit (CASA) program – sometimes referred to as a Desk Audit Program.

Initially created by Florida, **ASUS** has implemented its version of CASA on behalf of three (3) States, including Florida, Nevada and Louisiana.

Recognizing that conducting comprehensive audits of hundreds, or even thousands of smaller companies may not be practical or cost effective, **ASUS** has developed a process, further detailed in our proposal, whereby companies that have failed to report unclaimed property can be identified and procedures can be undertaken to support their compliance.

Sample procedures and materials (sample version most recently developed for the State of Nevada) are attached for your reference as ***ASUS Exhibit O – Contractor Assisted Self Audit.***

In summary, the CASA program includes the following steps:

- 1) Identify and load various databases aggregated from disparate systems and resources, and representing those industries and business types and sizes wherein unclaimed property is most likely to be generated.
- 2) Obtain, if possible, from the State a limited extract of the database of holders reporting to the State, normalize the form of this database to facilitate comparison, and likewise load this database to our system.
- 3) Using the **ASUS'** automated data matching algorithms, compare the known holders from the State's database with the potential holders in our aggregated database, and report those potential holders not currently reporting to the State for further review.
- 4) Complete a more detailed review of the resulting list of potential holders to eliminate false positives, duplicates, and other errata or anomalies.
- 5) Generate a report of the potential holders discovered in a form that will enable the State to determine whether to authorize a contractor-assisted self-audit.

- 6) Send notices, in coordination with the State, to the revised list of potential holders, to advise them of their obligation to report unclaimed property to the State, and of the procedures necessary for reporting.
- 7) After receipt of written authorization from the State, **ASUS** will conduct an opening conference or teleconference with the holder, and provide holder with an orientation/overview/instructions packet approved by the State.
- 8) Provide support for those potential holders who may have questions regarding these notices, and pro-actively contact potential holders until their potential obligation to confirm and/or report unclaimed property is resolved.
- 9) Obtain information from potential holders sufficient to determine whether a reporting obligation to the State exists, and prepare a preliminary estimate of the extent of the hitherto unreported unclaimed property.
- 10) **ASUS** will provide other necessary guidance and assistance to the holder so that the holder can accurately perform the self-audit. Once the holder has completed the self-audit and unclaimed property report, **ASUS** will review the report to verify its completeness, proper format and compliance, and then forward the report and remittance to the State.
- 11) For the holders identified by **ASUS** in the Identification process, and, optionally, for additional holders as may be referred to **ASUS** by the State, we will inform the holder or holder's agent of the requirements of the unclaimed property laws and details of the State's reporting requirements.

Enforcement Efforts

ASUS will endeavor to work with holders on a cooperative basis. While most holders will willingly permit a review or examination to proceed, there are those that may not be amenable to the process. In general, if a holder has a legitimate question or concern regarding the process, most issues can be resolved with a phone call or in person meeting. Where possible and necessary, State participation generally facilitates the negotiation process. For those holders that require more effort, an escalation process will be commenced. In addition to the required written notice to the State within fifteen (15) days of a holder's failure to report or deliver unclaimed property, an escalation process may also include:

- Conference call involving holder and representative from the State.
- A letter from **ASUS** requesting that the holder permit the review process to proceed and/or for the holder to put in writing its reasons for objecting to the process.

Responses will be developed with close consultation with the State and unclaimed property legal experts.

- A letter from the State to the holder requesting that the holder permit the review process to proceed and/or for the holder to put in writing its reasons for objecting to the process.
- A more strongly worded letter from the State outlining the consequences of non-compliance.
- Consultation with the State regarding compliance options.

4.1.3 Requesting Multi-State Audit Examinations: ASUS agrees with the requirements of this section and will comply accordingly. Prior to the commencement of any audit, ASUS will draft and submit electronically, to the Unclaimed Property Compliance Director, a request for audit. The request for audit should include the following information, if available. The auditor is not required to submit information regarding another state if confidential by law or by contract. Failure to provide sufficient information may result in the rejection of the audit.

4.1.3.1 All invited and participating states.

4.1.3.2 All Holders, including all subsidiaries or affiliated holders and the parent company, included in the scope of the audit, identified by both FEIN and Legal Name and any name they are doing business under.

4.1.3.3 The time period of records to be examined based upon the cutoff date. The cutoff date is defined by the property's last activity date.

4.1.3.4 An explanation of factors qualifying the Holder for audit.

4.1.3.5 Specific scope of types of records and/or transactions to be audited, including but not limited to:

A. Type of audit, as defined as, but not limited to:

1. General ledger audit – includes property other than securities. ASUS cannot classify an audit that includes a book review of securities as a general ledger audit. An audit that includes forms of ownership other than securities may still qualify as a general ledger audit, OR

2. Securities audit – includes only securities, OR
3. Full scope audit – includes all possible property types, OR
4. Virtual currency audit.

B. Parent company’s date of formation and date of incorporation.

C. Holder’s state of incorporation and principal place of business.

D. Indication of whether the holder currently or at any time previously has been located in, doing business in, or has been incorporated in West Virginia.

Our process for conducting an unclaimed property examination begins with a thorough research of the holder’s reporting history. To identify holders, we look for companies doing business in particular industries -- such as insurance, retail, utilities, banking, etc. -- where instances of unclaimed property typically occur. Companies in these categories that are flagged for further review include those that:

- do not report unclaimed property,
- submit reports indicating no unclaimed property to report,
- omit types of property typically found within the company's industry,
- or report amounts significantly at variance with industry norms.

Other considerations are companies involved in recent mergers or acquisitions, and companies in industries that typically employ a large transient workforce. In some cases we may also be asked by a state to audit specific holders already known to the state.

Pre-audit research may also include: assessing companies for annual revenue, number of employees, state of incorporation, overall market share and industry practices. Once information is gathered, the companies are typically compared to filing data supplied by various states. Once apparent non-compliance companies are identified, **ASUS** may send audit authorization requests to the State or one or more other states for approval. Typically, **ASUS** will solicit multiple, if not all states to join a general ledger audit. States will then have the opportunity to either initiate or join an audit that has already been initiated by one or more other states.

While audit recommendation criteria are defined in close consultation with our clients, our general guidelines may also include reviewing the following information:

- SIC Codes – is type or size of business of the audit candidate likely to give rise to unclaimed property?
- Annual Revenue - is the business large enough to generate material amounts of unclaimed property, sufficient to warrant the cost of an audit?
- Age of Business - has the business been in operation long enough to have property that has reached its dormancy period?
- Reporting History – is there evidence that would lead an objective reviewer to conclude that reporting has been complete and consistent?

Research data is gathered from publicly available sources such as: EDGAR filings, Dun & Bradstreet, Standard and Poor's and A.M. Best's.

ASUS acknowledges that the State reserves the right to participate in or restrict its participation in an audit of any holder.

Prior to beginning any audit, **ASUS** will draft and submit to the State an engagement letter (Sample **Authorization/Engagement Letter** attached set forth in ***ASUS Exhibit K – Sample Audit Authorization/Engagement Letter***) which defines agreed upon procedures, at a minimum:

- All holders, including all subsidiaries or affiliated holders, included in the scope of the audit, identified by both FEIN and Legal Name;
- Time period of records to be examined;
- Specific scope of types of records and/or transactions to be audited;
- Audit selection criteria used;
- Frequency and/or timing of reporting identified unclaimed property during an audit;
- Anticipated begin date of audit; and
- Anticipated time to complete audit;

A sample Holder Profile is set forth in ***ASUS Exhibit P – Sample Holder Profile***.

- 4.1.4** The **STO** may request **ASUS** to conduct a West Virginia state specific audit of an entity or evaluate if a multistate audit is beneficial. The audit examination process and procedures will be consistent with multistate audit authorizations.

ASUS acknowledges that the **STO** may request **ASUS** to conduct a West Virginia state specific audit of an entity or evaluate if a multistate audit

- 4.1.5 Audit Authorization:** **ASUS** agrees with the requirements of this section and will comply accordingly. Prior to commencing an audit, **ASUS** will obtain written approval in the form of a standardized Authorization Letter approved by the **STO**, on **STO** letterhead. The **STO** has the final and sole authority to determine who, if anyone, will conduct an examination of Holders. All unclaimed property funds or securities submitted by **ASUS** or the Holder pursuant to an examination conducted without an Authorization Letter from the **STO** shall be received by the **STO** without compensation to **ASUS**. The **STO** will advise **ASUS** of a rejected audit examination request within sixty (60) days of the initial request.

The **STO** reserves the right to require the Audit Guidelines described in Section 4.1.1 be included as an attachment with the Authorization Letter.

- 4.1.6 Multi-state Audit Authorizations:** **ASUS** agrees with the requirements of this section and will comply accordingly. In the event of multi-state audits, and if in agreement with some or all participating states, **ASUS** will request and receive approval from a majority of participating states prior to initiation of the audit, if possible. The authorization letters will be sent in a single batch or minimal batches from all states that are in agreement with this process to serve as notice to the Holder of the initiation of the multi-state audit and as a signal of uniformity by the participating states.

- 4.1.7 Authority:** **ASUS** agrees with the requirements of this section and will comply accordingly. As stated in our Executive Summary, **ASUS** recognizes that the States it serves govern its actions, and it has the responsibility to follow the instructions of the client State for the various services provided, as well as complies with all federal, state and local laws that may apply. We recognize that in the absence of holder records that **STO** approval will be required before applying estimation techniques to determine the amount of unclaimed property that should be demandable.

4.1.8 Timeframe: **ASUS** agrees with the requirements of this section and will comply accordingly. **ASUS** also recognizes the need to complete unclaimed property examinations in a timely and efficient manner, and our auditors are trained to adhere to our audit procedures to ensure this occurs. It is our policy to open and engage in no more examinations than we feel we can handle within a prescribed time frame, and the examination should be commenced no later than ninety (90) days after the notification to **ASUS** of the assignment of the examination, except on a showing of good cause. In the event there is a scheduling conflict or problems with providing records, **ASUS** will work with the holder to resolve these issues. In any case, the State will also be notified of any changes.

Audits shall be authorized for **three (3) years** from the date of the authorization letter. Should the auditor not complete the audit in that time, they shall request an extension of the audit. Extension may be granted in one (1) year increments. If an extension is not received at least forty-five (45) days prior to the expiration of the audit, the extension request may not be reviewed, and the audit will set to expire. Unless extenuating circumstances are adequately demonstrated, no more than one (1) extension may be granted under any audit.

4.1.9 Act Requirements and Notices: As an unclaimed property auditing services provider to West Virginia for over twenty-two (22) years, **ASUS** has successfully completed hundreds of audits on behalf of and reported over \$4.1 million to the state over the past ten (10) years. We believe that the combination of our highly experienced personnel, with our proven track record in West Virginia, **ASUS** demonstrates its knowledge, ability and commitment to comply with West Virginia's unclaimed property law, and all federal legislation and court rulings regarding the Uniform Unclaimed Property Act. **ASUS** agrees with the requirements of this section and will comply accordingly. It is our policy to advise each holder of meeting the unclaimed property law requirements for each State we represent. Prior to making demand from the holder for unclaimed property that is due and payable to our contract states, due diligence by the holder must be performed. **ASUS's** auditors are well versed in the different State laws and will advise holders regarding the provisions of the State's laws and the requirements for performing due diligence in making attempts to locate the rightful owner before property is remitted as unclaimed. Since we have established as one of our performance benchmarks the necessity of performing due diligence, our auditors conduct a review of due diligence between the potential findings stage and the final findings stage of the examination. Due diligence can be done solely by the holder, or with our assistance. If required, certifications to the completion of the due diligence requirements will be obtained from the holder prior to the balance of the property being remitted to the State as unclaimed. **ASUS** will advise each Holder of the requirements

of W.VA. Code §36-8-7 for notifying owners of their property (“Due Diligence”) and will notify the ST if the Holder failed to conduct Due Diligence. **ASUS** will also advise Holders that all property reported and remitted must conform to the requirements of the Act, now and in the future. **ASUS** will advise each Holder of the NAUPA reporting format and the required information for its use. **ASUS** will advise each Holder of record retention requirements under W.VA. Code §36-8-21. Holders are not exempt from any section of the Act, including but not limited to W.VA. Code §36-8-24, which grants the **STO** the authority to charge penalties and interest to delinquent Holders. **ASUS** will not represent to Holders that penalties and interest will be waived without written authorization from the **STO**.

4.1.10 Bankruptcy of Holder: **ASUS** agrees with the requirements of this section and will comply accordingly. **ASUS** will notify the **STO** if it is discovered a Holder has filed for bankruptcy. **ASUS** will provide all available information to the Unclaimed Property Compliance Director within seven (7) days of discovery of the pending bankruptcy by **ASUS**.

4.1.11 Closure: **ASUS** acknowledges it must properly close an audit, as required by the requirements listed herein. After the Holder and **ASUS** have agreed to the amount deliverable, **ASUS** will provide the Holder and the **STO** with a final examination report summarizing the procedures performed and the conclusions reached, including the amount deliverable. **ASUS** will properly close the audit on the following month’s Work-In-Progress Report (“WIP”). If applicable, the **STO** will notify the Holder of any interest or penalties assessed on delinquent property.

ASUS agrees with the requirements of this section and will comply accordingly. It is **ASUS**’s policy to make demand of a Holder for remittance of property to the State only after we have reconciled and agreed with the Holder on the report to be filed with the State Treasurer’ Office. In the event **ASUS** and the Holder do not agree upon the report to be filed, the State Treasurer’s Office will decide the matter. **ASUS** will properly close the audit on the following month’s Work-In-Progress Report (“WIP”). If applicable, the **STO** will notify the Holder of any interest or penalties assessed on delinquent property.

4.1.12 Reporting: **ASUS** agrees that in conjunction with the identification and collection of unclaimed property, in either voluntary or involuntary examinations, we shall comply with the requirements described below.

4.1.12.1 Process records of unclaimed property obtained from Holders and/or their agents. **ASUS** will process records of unclaimed property obtained from Holders and/or their agents.

4.1.12.2 Timely submit all required reports and notices electronically to the Unclaimed Property, Compliance Director. **ASUS** will timely submit all required reports and notices to West Virginia State Treasurer's Unclaimed Property Division, 322 70th Street SE, Charleston, WV 25304.

4.1.12.3 Prepare and submit to the **STO** reports of unclaimed property in accordance with the requirements of the Act & corresponding West Virginia legislative rule, 112 CSR 5. **ASUS** will prepare and submit to **STO** reports of unclaimed property in accordance with the requirements of the Unclaimed Property Act and corresponding legislative rule, 112 CSR 5.

Property will be transferred in trust for the **STO** to one of our custodians, Signature Bank for cash deliveries and Mellon Securities Trust Company for securities, or remitted directly to the **STO** by the holder. If submitted to our custodian, the property will be held in an escrow account, earning interest on behalf of the State at the prevailing market rate. Securities will be registered as directed by the contract, and remitted to Audit Services to be held by our custodian or, if possible, transferred to the State through DTC.

4.1.12.4 Report all unclaimed property electronically using the NAUPA II standardized unclaimed property reporting format. It is **ASUS's** policy to file an unclaimed property report and invoice with the remittance when an examination is completed. All raw data obtained from the examination is input (physical or download) into our own proprietary software (*See ASUS Exhibit L – The Audit Services System*). The *Audit Services System* software allows our Company to file a “hard copy” report to West Virginia as well as a report in a standard NAUPA II standardized unclaimed property reporting format. The *Audit Services System* is compliant with all 50 states' requirements and utilizes the NAUPA standard reporting format, among others for reporting unclaimed property to client states. We recognize that providing accurate and precise information that can be downloaded to our client State's database is essential to the processing of data received in a timely and efficient manner. This information is necessary for not only accounting purposes, but to facilitate the possibility of the State locating the rightful owner.

4.1.12.5 Timely submit, pay or deliver all funds and other property constituting unclaimed property to the **STO**, or its designee subsequent to the processing of the Holder's records and **ASUS's** demand of report and payment or delivery, as provided in this subparagraph.

All funds, must be segregated and securely maintained by ASUS for a period not to exceed thirty (30) calendar days prior to disbursement to the **STO** or its designee. It is our policy that once an examination is completed and reconciled, the property identified will be remitted to the State within 30 days. Details regarding the ASUS cash and securities custodian follow below:

Custodian of Cash and Securities

Property will be transferred in trust for the to one of our custodians, SIGNATURE BANK or MELLON SECURITIES TRUST COMPANY as shown below, or remitted directly to the **STO** in accordance with the requirements of the RFQ, by the holder after reconciliation is complete. Delivery of the property will be no more than thirty (30) days from the completion of the audit.

For cash property, ASUS utilizes:

Name: **SIGNATURE BANK**

Address: **50 WEST 57th STREET, NEW YORK, NY 10019**

Contact Person: **BRIAN J. HALLINAN**
GROUP DIRECTOR-SENIOR VICE PRESIDENT

Telephone: **(646) 495-4694**

For security-related property, ASUS utilizes:

Name: **BNY MELLON SECURITIES CORPORATION**

Address: **240 GREENWICH STREET, NEW YORK, NY 10007**

Contact Person: **SIDDHARTH SARASWAT**
VICE PRESIDENT

Telephone: **(646) 782-4160**

4.1.13 Securities: ASUS agrees with the requirements of this section and related subsections and will comply accordingly. Securities will be registered and delivered as directed by the State. Shares will generally be remitted to ASUS and briefly held in our custody account in preparation for transfer to the State's custodian through DTC. Non-DTC eligible securities will be delivered in certificated form per the State's registration instructions. ASUS utilizes Mellon Securities Trust Company located in New York, NY, for securities custody. Whether general ledger property or securities related, the property will be remitted to the custody of the State within thirty (30) days from receipt or reconciliation.

4.1.13.1 ASUS shall cause all securities to be re-registered to the State of West Virginia or its nominee, as directed by the STO, and delivered using Depository Trust Company (DTC) designations when applicable. For all securities that are not DTC eligible, ASUS will cause them to be re-registered to the WV State Treasurer or its nominee, at the written direction of the STO, and delivered in physical form to the STO, or its designee. Worthless securities will not be reported or transferred to the STO.

4.1.13.2 The accompanying invoice will include the value of the shares on the date the property is received by the STO. The value of any security shall be the closing price of that security on the date the property is received by the STO or the STO's custodian. If the property is a security traded over the counter, it shall be the bid price as set forth in the over the counter market. For any other security related properties, the value will be determined according to generally accepted valuation procedures. A sample invoice is set forth in *ASUS Exhibit Q – Sample Invoice*.

4.1.14 Demands for Remittance: ASUS agrees with the provisions of this section. ASUS is capable and able to demand and accept remittances of unclaimed property from Holders. Unless otherwise authorized by the STO, ASUS will not make a demand of a Holder for remittance of property to the STO until such time as the Holder and ASUS reconcile and agree upon the report to be filed with the STO. In the event ASUS and Holder do not agree upon the report to be filed, ASUS will notify the STO, who shall decide the matter.

4.1.15 Dispute Resolution: ASUS agrees with the requirements of this section and will comply accordingly. ASUS recognizes that occasionally timely disbursement of property may be delayed as a result of a dispute with respect to the delivery, ownership, right of possession and/or disposition of property. We will notify the STO of any such disputes within thirty

(30) days of determination that a dispute exists. In addition, we will make all reasonable efforts to resolve any disputes as quickly as possible. In the event **ASUS** and the Holder are unable to reach an agreement as to the terms of **ASUS**'s final examination report, the Holder may maintain an original action to establish the claim in the circuit court of Kanawha County, naming the administrator as a defendant.

4.1.16 Property Disputes: Vendor will be able to assist the **STO** with property disputes. **ASUS** agrees with the requirements of this section and will comply accordingly. Timely disbursement of property may be delayed because of a dispute with respect to the delivery, ownership, right of possession and/or disposition of property. Delivery requirements may be suspended at the discretion of the **STO** pending resolution of said disputes or as otherwise requested by the **STO**. **ASUS** shall notify the **STO** of any such disputes within thirty (30) days of determination that a dispute exists. **ASUS** will then make all reasonable efforts to resolve disputes as quickly as possible. **ASUS** will provide to the **STO** the actual resolution date of any such disputes and will remit the property within thirty (30) days of resolution of disputes.

4.1.17 Release Agreements: Vendor must prepare Release Agreement according to **STO** procedures. **ASUS** agrees with the requirements of this section and will comply accordingly. As stated in our Executive Summary, it is our policy to provide release agreements when requested by the Holder, identifying the property records to be submitted, and signed by the holder and the West Virginia State Treasurer's Office. **ASUS** will prepare a Release Agreement, when requested by a Holder, to be signed by the Holder and the **STO**, which shall identify the property to be remitted, and verify that the appropriate abandonment period has been met for each type of property reported. A copy of a sample *Standard Release Agreement* is attached as **STO Exhibit C- Standard Release Agreement**. The **STO** reserves the right to modify the terms of the Release Agreement at its discretion.

4.1.18 Work-In-Progress Reports: **ASUS** will provide to the **STO** Work-In-Progress Reports ("WIPs") according to the following procedures:

4.1.18.1 **ASUS** will provide the Unclaimed Property Compliance Director at UP_Compliance@wvsto.com, by the 15th of each month, for the previous month, a WIP for each Holder under examination. All Holders under audit must be listed in the WIPs from the time the audit is commenced until the audit is formally closed. The WIPs will be in the form of and include all information required by the current sample Work-In-Progress

Report Template attached as ***STO Exhibit D – Work-In-Progress Report Template***. This template may be amended at the written discretion of the **STO**.

ASUS agrees with the requirements of this section and will comply accordingly. To keep the State current on the progress of our audits, **ASUS** issues a monthly work-in-progress report (***ASUS Exhibit R- Work-In-Progress Report***), by the 15th of each month. **ASUS's** monthly work-in-progress report provides the state with an alphabetical listing of all holders who are currently under audit. Included in the report is the holder's FEIN, the audit start date, the audit period covered, the types of property being audited and a comments field to describe the status or progress of the audit. The work-in-progress report can be modified to meet the requirements of the State.

4.1.19 Review and Retention of Records: **ASUS** must permit the **STO** to review all records it maintains to ensure **ASUS's** compliance with all the terms and conditions of the purchase order issued pursuant to this RFQ. The scheduling of these reviews will be designated by the **STO**. All working papers and reports must be retained, at **ASUS's** expense, for a minimum of ten (10) years from the originating date, unless **ASUS** is notified in writing by the **STO** to extend the retention period.

ASUS agrees with the requirements of this section and will comply accordingly. Upon the completion of an examination, **ASUS** will maintain the records and supporting documentation from the examination for a minimum of ten (10) years. All information obtained in the course of an examination will be made available to the contracting state if requested by the State.

4.1.20 Joint Examinations: **ASUS** agrees the **STO** reserves the right to participate in a joint examination of any Holder, at any time, with **ASUS**.

ASUS agrees with the requirements of this section and will comply accordingly. **ASUS** welcomes the State of West Virginia to participate in any examination in progress.

4.1.21 Fees: **ASUS** agrees to payment for audit services as follows:

4.1.21.1 Except as provided in Section 4.2.10 and Section 4.3.1 below, all **ASUS** fees for the identification and collection of unclaimed property will be the lesser of a flat **10.5** percent (**10.5%**) of the net unclaimed property remitted to the **STO**, or the lowest fee percentage charged to any other state for the same Holder multi-state audit, less any interest

due pursuant to the provision of this RFQ. In such case, if the fee is lower than **10.5%**, **ASUS** will provide written notice of the lower fee and agree to provide the same fee.

4.1.21.2 Net unclaimed property is the gross value of all unclaimed property, minus the value of all unclaimed property delivered by the Holder, if any, that otherwise would have been delivered pursuant to the reporting practices of the Holder as they existed prior to the execution of the agreement with **ASUS**. Payment will be made in arrears, based upon invoices submitted by **ASUS**, once property is received.

4.1.21.3 Failure to deliver property to the **STO** within thirty (30) days of receipt from the Holder will result in the following reductions in fees, unless a dispute occurs or unless the **STO** waives the reduction for matters beyond the reasonable control of **ASUS**. The **STO** reserves the right to request documentation indicating the date the property was received by **ASUS**. **ASUS** must provide requested information within two (2) business days of request.

4.1.21.3.1 Audit reports, funds and securities that are submitted thirty-one (31) to sixty (60) calendar days after the receipt of property by **ASUS** or its designee may be subject to up to a 33% fee reduction, at the discretion of the **STO**.

4.1.21.3.2 Audit reports, funds and securities that are submitted sixty-one (61) to ninety (90) calendar days after receipt of property by **ASUS** or its designee may be subject to up to a 66% fee reduction, at the discretion of the **STO**.

4.1.21.3.3 Audit reports, funds and securities that are submitted past ninety-one (91) calendar days after the receipt of property by **ASUS** may be considered past due and may result in a forfeiture of the entire fee, at the discretion of the **STO**. The **STO** reserves the right to require **ASUS** to submit all reports and property immediately upon reaching past due status.

ASUS agrees with the requirements of this section and related subsections and will comply accordingly. We acknowledge that the fee for the identification and collection of unclaimed property will be a flat 10.0% of the net unclaimed property remitted to the State Treasurer's Office, less any interest due pursuant to the provisions of the RFQ. For those examinations requiring alternate reasonable compensation, **ASUS** will be paid on an hourly basis at the rate of \$100 per hour. **ASUS** recognizes that it is responsible for the payment or making provision for the payment of all expenses incurred in connection with all services provided in the RFQ.

4.1.22 Confidentiality: All matters dealing with the contract between **ASUS** and the State will be maintained in strict confidence. Also, any information obtained from the holder or the State Treasurer's Office is considered proprietary and confidential in nature and will not be disclosed to a third party. If it is felt that the information would be beneficial in the conduct of an unclaimed property examination on behalf of another State, this information can be released to another State.

4.2 ADDITIONAL OPTIONAL SERVICES WHICH VENDOR MAY PROVIDE

4.2.1 Additional Services: Vendor Assisted Self Audit: See the **ASUS** Contractor Assisted Self Audit Program referenced in Section 4.1 above and as set forth in ***ASUS Exhibit O – Contractor Assisted Self Audit.***

4.2.2 Assistance: **ASUS** will assist the **STO** in the identification, outreach, education, and notification of potential Holders of unclaimed property. **ASUS** will assist in the education of the Holders' obligation to file unclaimed property reports and to remit those funds to the **STO**.

4.2.3 Identification: **ASUS** will research and identify potential Holders of unreported unclaimed property that is past due. **ASUS** will provide written justification for seeking approval for Holder to participate in this program. The **STO** may also identify potential Holders and request their participation in the program.

4.2.3.1 Written Justification: **ASUS's** written justification must be based on the Holder's reporting history and an indication of the Holder's willingness to be compliant with the Act.

4.2.3.2 Review Plan: Vendor-assisted self-review plan will identify **ASUS's** staff and the assistance that will be provided to the Holder, an expected timeline to begin with an opening conference and conclude with a closing conference, the general methods to be employed and the time period to be covered by the vendor-assisted self-review.

4.2.4 Authorization: **ASUS** will obtain prior written authorization from the **STO** to oversee a self-audit of a Holder under this program. The **STO** has the final and sole authority to determine who, if anyone, will take part in the self-audit and will also make

requests in writing to **ASUS**. All unclaimed property funds or securities submitted by **ASUS** or the Holder pursuant to any self-review under this program conducted without prior written approval from the **STO** shall be received by the **STO** without compensation to **ASUS**.

4.2.5 Vendor-Assisted Self-Audit: Within ninety (90) days of obtaining authorization from the **STO**, **ASUS** will contact the Holder and begin to execute Vendor-assisted self-review plan. **ASUS** will assist the Holder to determine, report, and collect all types of unclaimed property in the possession of the Holder, within the scope of the audit due and owing the **STO**. **ASUS** will explain its responsibilities to the Holder which will include the following phases:

ASUS will gather and document basic corporate information;

- **ASUS** will review the financial statements in order to advise the Holder of the types of property to be included in the self-review;
- **ASUS** will review the self-review analysis prepared by the Holder;
- **ASUS** will assist the preparation of the unclaimed property report;
- **ASUS** will prepare a final report to close the self-review, and
- **ASUS** will review the Holder's final report and submit the final report and remittance to the **STO**.

4.2.6 Timeframe: The self-review of the Holder's records under the Compliance Program will be completed within one (1) year from the date of the **STO's** authorization letter unless the **STO** grants an extension.

4.2.7 Work-In-Progress: **ASUS** will submit regular WIPs on all pending vendor-assisted self-reviews in an electronic format previously agreed upon prior to authorization. These may be in a format which differs from Section 4.1.19.

4.2.8 Collection and Delivery: **ASUS** will report all property remitted in accordance with Section 4.1.12 and 4.1.13 as required by Section 4.1.17. The Holder will deliver any tangible property such as contents of safe deposit boxes directly to the **STO**.

4.2.9 Education and Compliance: Prior to closing the vendor-assisted self-review, ASUS will educate the Holder on its future compliance with the Act including those requirements noted in Section 4.1.9.

4.2.10 Compensation: All Vendor fees for the Voluntary Compliance Program will be a flat **nine percent (9%)** of the net unclaimed property remitted to the **STO**. Net unclaimed property is the gross value of all unclaimed property, minus the value of all unclaimed property delivered by the Holder, if any, that otherwise would have been delivered pursuant to the reporting practices of the Holder as they existed prior to the execution of the agreement with **ASUS**. Payment will be made in arrears, based upon invoices submitted by **ASUS**, once property is received.

4.3 Additional Services: Vendors with the minimum qualifications set forth in Section 3 may be selected to conduct agreed upon procedures related to a Holder that may or may not have been part of an audit. If selected, the scope of the Agreed Upon Procedure will be outlined in a delivery order.

4.3.1 Compensation: Audit Agreed Upon Procedures related to a Holder which is outside of the scope of a multistate audit, West Virginia state specific audit, or Vendor-assisted self-audits will be paid on an hourly basis at the rate of **\$100 per hour**, and the total cost will be capped in a release order, if selected.

ASUS agrees with all of the requirements of this Request for Quotation. Items to which we did not make a specific response were considered not to be required, however all items were reviewed, understood and accepted.

5. CONTRACT AWARD

- 5.1 Contract Award:** The Contract is intended to provide the **STO** with a purchase price for the Contract Services. The Contract may be awarded to all Vendors that provide the Contract Services meeting the required specifications.

ASUS acknowledges and understands that the Contract is intended to provide the **STO** with a purchase price for the Contract Services. Furthermore, **ASUS** acknowledges and understands the Contract may be awarded to all Vendors that provide the Contract Services meeting the required specifications.

- 5.2 Pricing Page:** **ASUS** acknowledges and accepts the set reimbursement fees listed in subsections 4.1.21, 4.2.10, and 4.3.1 and has completed the Pricing Page (**Exhibit A**) in full.

ASUS will type or electronically enter the information into the Pricing Page through wvOASIS, if available, or as an electronic document.

EXHIBIT A – PRICING PAGE (REVISED)

ASUS will offer this service: Yes ✓ No

REQUEST FOR QUOTATION
Professional Auditing Services

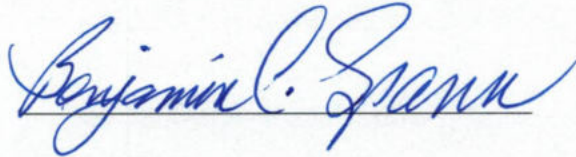
I/We agree to the established fee schedule for the mandatory services listed within this solicitation and resultant contract award, including any of the selected optional services affirmed above:

Company Name: **Audit Services U.S., LLC**

Printed Name of Signatory: **Benjamin C. Spann**

Title of Signatory: **Chief Executive Officer**

Signature:

A handwritten signature in blue ink, reading "Benjamin C. Spann", written over a horizontal line.

6. PERFORMANCE: ASUS and STO shall agree upon a schedule for performance of Contract Services and Contract Services Deliverables, unless such a schedule is already included herein by STO. If this Contract is designated as a Master Agreement, ASUS shall perform in accordance with the delivery orders that may be issued against this Contract.

7. PAYMENT: Agency shall pay in accordance with all authorized Contract Services requested and accepted by the STO under this Contract. ASUS shall accept payment in accordance with the payment procedures of the State of West Virginia. All services are paid in arrears upon presentment of an approved invoice and any required supporting documentation.

8. TRAVEL: ASUS will be responsible for all mileage and travel costs, including travel time, associated with performance of the Contract. Any anticipated mileage or travel costs may be included in the flat fee or hourly rate listed on ASUS's bid, but such costs will not be paid by the Agency separately.

9. FACILITIES ACCESS: Performance of Contract Services may require access cards and/or keys to gain entrance to Agency's facilities. In the event that access cards and/or keys are required:

- 9.1.** ASUS must identify principal service personnel which will be issued access cards and/or keys to perform service.
- 9.2.** ASUS will be responsible for controlling cards and keys and will pay replacement fee if the cards or keys become lost or stolen.
- 9.3.** ASUS shall notify Agency immediately of any lost, stolen, or missing card or key.
- 9.4.** Anyone performing under this Contract will be subject to Agency's security protocol and procedures.
- 9.5.** ASUS shall inform all staff of Agency's security protocol and procedures.

10. VENDOR DEFAULT

10.1. The following shall be considered a vendor default under this Contract.

10.1.1. Failure to perform Contract Services in accordance with the requirements contained herein.

10.1.2. Failure to comply with other specifications and requirements contained herein.

10.1.3. Failure to comply with any laws, rules, and ordinances applicable to the Contract Services provided under this Contract.

10.1.4. Failure to remedy deficient performance upon request.

10.2. The following remedies shall be available to Agency upon default.

10.2.1. Immediate cancellation of the Contract.

10.2.2. Immediate cancellation of one or more release orders issued under this Contract.

10.2.3. Any other remedies available in law or equity.

11. MISCELLANEOUS

- 11.1 Contract Manager: During its performance of this Contract, **ASUS** must designate and maintain a primary contract manager responsible for overseeing **ASUS's** responsibilities under this Contract. The dedicated Contract Manager must have experience in providing audit services and must be available during normal business hours to address any customer service or other issues related to this Contract. If it becomes necessary for **ASUS** to change the Contract Manager, **ASUS** must notify the **STO** immediately. The replacement must have similar or more experience than the original Contract Manager. The **STO** reserves the right to approve any replacement at the time of the contract award or thereafter. **ASUS** should list its Contract Manager and this person's contact information below.

Contract Manager: **Benjamin C. Spann**

Telephone Number: **(225) 324-0139**

Fax Number **(212) 594-5571**

Email Address: **bspenn@auditservicesus.com**

WVSTO Exhibit A

Pricing Page

EXHIBIT A – PRICING PAGE (REVISED)

ASUS will offer this service: Yes ✓ No

REQUEST FOR QUOTATION
Professional Auditing Services

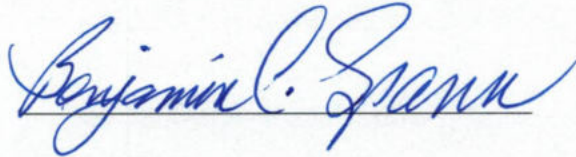
I/We agree to the established fee schedule for the mandatory services listed within this solicitation and resultant contract award, including any of the selected optional services affirmed above:

Company Name: **Audit Services U.S., LLC**

Printed Name of Signatory: **Benjamin C. Spann**

Title of Signatory: **Chief Executive Officer**

Signature:

A handwritten signature in blue ink, reading "Benjamin C. Spann", written over a horizontal line.

WVSTO EXHIBIT B

West Virginia
Property Type Codes



UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

WV Property Type Codes

Effective June 10, 2022

CODE	PROPERTY	YEARS
BANKS & FINANCIAL INSTITUTIONS		
AC01	Checking Accounts	5
AC02	Savings Accounts	5
AC03	Mature CD or Save Cert	5
AC04	Christmas Club Accounts	5
AC05	Money on deposit to secure funds	5
AC06	Security Deposits	5
AC07	Unidentified Deposits	5
AC08	Suspense Accounts	5
AC99	Aggregate Account balances	5
COLLEGE SAVINGS ACCOUNTS		
CS01	Cash	3
CS02	Mutual Funds	3
CS03	Securities	3
COURTS & GOVERNMENT ENTITIES		
CT01	Escrow Funds	1
CT02	Condemnation Awards	1
CT03	Missing Heir Funds	1
CT04	Suspense Accounts	1
CT05	Other Court Deposits	1
CT08	General Receiver accounts	1
CT09	Court Ordered Refunds/Restitution	1
CT13	Bonds deposited with the Court	1
CT99	Aggregate Court Deposits	1
DEMUTUALIZATION		
DM01	Cash	3
DM02	Stock	5
HEALTH SAVINGS ACCOUNTS		
HS01	Health Savings Account	3
HS02	Health Savings Account – Investment	3
INSURANCE		
IN01	Individual Policy Benefits or Claim Payments (Regardless of insurance type; does not include amounts reportable under IN03 or IN04)	3
IN02	Group Policy Benefits or Claim Payments (Regardless of insurance type; does not include amounts reportable under IN03 or IN04)	3
IN03	Amounts due beneficiaries from a life or endowment insurance policy or annuity	3
IN04	Amounts from matured or terminated life insurance policies, endowments or annuities	3
IN05	Premium Refunds (Includes all other life insurance premium refunds not covered by IN04)	3
IN06	Unidentified Remittances	3
IN07	Other Amounts Due Under Policy Terms	3
IN08	Agent Credit Balances	1
IN99	Aggregate Insurance Property	3
TRADITIONAL IRA, SEP IRA, SARSEP IRA AND SIMPLE IRA'S		
IR01	Cash	3
IR02	Mutual Funds	3
IR03	Securities	3
ROTH IRA'S		
IR05	Cash	3
IR06	Mutual Funds	3
IR07	Securities	3
LAW ENFORCEMENT		
LE01	Law Enforcement - Cash	6 months
LE98	Law Enforcement – Tangibles	6 months





UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

CODE	PROPERTY**	YEARS
MINERAL PROCEEDS AND MINERAL INTERESTS		
MI01	Net Revenue Interests	3
MI02	Royalties	3
MI03	Overriding Royalties	3
MI04	Production Payments	3
MI05	Working Interests	3
MI06	Bonuses	3
MI07	Delay Rentals	3
MI08	Shut-in Royalties	3
MI09	Minimum Royalties	3
MI99	Aggregate Mineral Proceeds	3

MISCELLANEOUS CHECKS AND INTANGIBLE PERSONAL PROPERTY		
MS01	Wages, payroll, or salary	1
MS02	Commissions	1
MS03	Workers' Compensation Benefits	1
MS04	Payments for Goods and Services	3
MS05	Customer Overpayments/Credit Balances--Retail only	3
MS06	Unidentified Remittances	3
MS07	Unrefunded Overcharges	3
MS08	Accounts Payable	3
MS09	Credit Balances/Accounts Receivable	3
MS10	Discounts Due	3
MS11	Refunds due	3
MS12	Unredeemed Gift Certificates	3
MS13	Unclaimed Loan Collateral	3
MS14	Pension and Profit Sharing Plans (IRA, KEOGH, e.g.)	3
MS15	Dissolution or Liquidation Funds	1
MS16	Miscellaneous Outstanding Checks	3
MS17	Miscellaneous Intangible Property	3
MS18	Suspense Liabilities	3
MS99	Aggregate Misc Property	3

SAFE DEPOSIT BOXES AND SAFEKEEPING		
SD01	Contents of safe deposit boxes	5
SD02	Contents of any other safekeeping repository	5
SD03	Other Tangible Property	5
SD04	Safe Deposit - Proceeds from the sale of contents	5

SECURITIES		
SC01	Dividends	5
SC02	Interest (Bond Coupons)	5
SC03	Bond Principal	5
SC04	Equity Payments	3
SC05	Profits	3
SC06	Funds Paid to Purchase Shares	3
SC07	Funds for Stocks and Bonds	3
SC08	Shares of Stock (returned by post office)	5
SC09	Cash for Fractional Shares	3
SC10	Unexchanged Stock of Successor Corporation	5
SC11	Other Certificates of Ownership	5
SC12	Underlying Shares	5
SC13	Funds for Liquidation/Redemption of Unsurrendered Stocks or Bonds	3
SC14	Debentures	3
SC15	U.S. Government Securities	5
SC16	Mutual Fund Shares	5
SC17	Warrants (Rights)	3
SC18	Mature Bond Principal	5
SC19	Dividend Reinvestment Plans	5
SC20	Credit Balances	3
SC21	Liquidated Mutual Fund Shares	3
SC99	Aggregate Security Related Cash	3





UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

CODE	PROPERTY**	YEARS
TRUST, INVESTMENTS, AND ESCROW ACCOUNTS		
TR01	Paying Agent Accounts	3
TR02	Undelivered or Uncashed Dividends	3
TR03	Funds held in Fiduciary Capacity (such as, trust, guardian, estate, etc.)	3
TR04	Escrow Accounts	3
TR05	Trust Vouchers	3
TR99	Aggregate Trust Property	3
UNCASHED CHECKS		
CK01	Cashier's Checks	3
CK02	Certified Checks	3
CK03	Registered Checks	3
CK04	Treasurer's Checks -- West Virginia Checks (6 Month Dormancy), All Other Checks (3 Year Dormancy)	6 ms or 3
CK05	Drafts	3
CK06	Warrants	3
CK07	Money Orders -- Financial Institutions (3 Year Dormancy), Entities other than Financial Institutions (7 Year Dormancy)	3 or 7
CK08	Traveler's Checks	15
CK09	Foreign Exchange checks	3
CK10	Expense Checks	3
CK11	Pension Checks	3
CK12	Credit Checks or Memos	3
CK13	Vendor Checks	3
CK14	Checks Written off to Income or Surplus	3
CK15	Other Outstanding Official Checks or Exchange Items	3
CK16	CD Interest Checks	3
CK99	Aggregate Uncashed Checks	3
UTILITIES		
UT01	Utility Deposits	1
UT02	Membership Fees	1
UT03	Refunds or Rebates	1
UT04	Capital Credit Distributions	3
UT99	Aggregate Utilities	1
Virtual Currency		
VC02	Virtual Currency Liquidated	3

Public Agencies - Use the most applicable property type code and report all property with one (1) year dormancy.



WVSTO EXHIBIT C

Standard
Release
Agreement

Exhibit C

STANDARD RELEASE AGREEMENT

This Standard Release Agreement ("Agreement"), effective the _____, 20__, is made by and between the West Virginia Office of the State Treasurer, Unclaimed Property Division ("the STO") and _____ (the "Holder").

WHEREAS, _____ on behalf of the West Virginia Office of the State Treasurer, Unclaimed Property Division, has performed an unclaimed property examination, pursuant to the provisions of West Virginia Unclaimed Property law to determine the Holder's compliance with the West Virginia Unclaimed Property law (the "Unclaimed Property Law"), and

WHEREAS, based upon the results of the examination, _____ has reported and remitted to the State on behalf of the Holder certain funds, securities and other intangible property that constitute unclaimed property pursuant to the Unclaimed Property Law, and

WHEREAS, the Holder recognizes that the Unclaimed Property Law requires that apparent owners of certain types and amounts of property be notified within a specified time period that the Holder is in possession of property subject to the Unclaimed Property Law, and

WHEREAS, the Holder certifies that is has complied with those notice requirements of the Unclaimed Property Law, and has complied with the remaining provisions of the Unclaimed Property Law;

NOW, THEREFORE, THIS AGREEMENT WITNESSETH:

The parties covenant and agree follows:

1. **Compliance:** Based upon the Holder's certification as to its compliance with Unclaimed Property Law notice and abandonment period requirements, and based upon the reporting and remitting of the identified property to the STO, the STO acknowledges that the Holder has complied with the provisions of the Unclaimed Property Law, with regard to the property reported. The identified property, if any, is listed on the attached Schedule A.
2. **Release:** In consideration of the good faith reporting and remitting of the identified property to the STO, the STO releases the Holder, and if applicable, any transfer agent, dividend or interest disbursing agent, or registrar, from any liability arising hereafter with respect to the reported and remitted property, pursuant to the Unclaimed Property Law. In further consideration of the good faith reporting and remitting of the identified property, the STO agrees to waive any applicable interest and penalties which might otherwise be imposed pursuant to Unclaimed Property Law.
3. **Reimbursement:** The STO further agrees to reimburse the Holder pursuant to the requirements of the Unclaimed Property Law in the event that any person or entity claims property previously delivered by the Holder to the STO, provided the property was reported and remitted to the STO in good faith, and provided that the Holder files proof of payment and proof that payee was entitled to the payment.
4. **Governing Law:** The laws of the State of West Virginia and the legislative rules of the STO shall govern all rights and duties under this agreement, including without limitation

Exhibit C

the validity of this agreement. In the event a lawsuit is brought involving this Release Agreement, venue shall be proper only in Circuit Court of Kanawha County, West Virginia. The parties hereby acknowledge jurisdiction of the courts of the State of West Virginia for purposes of this Agreement.

5. **Severability:** If any provision of this Agreement or any document referenced in this Agreement is found to be invalid by a court of competent jurisdiction, such invalidity shall not affect the remaining provisions which can be given effect without the invalid provision, and to this end, the provisions of this Agreement and any document referenced in the Agreement are declared to be servable.
6. **Effective date:** This release agreement shall be effective as of the date of the last signature.

WITNESS THE FOLLOWING SIGNATURES:

**West Virginia Office of State Treasurer
Unclaimed Property Division**

Holder

By: _____

By: _____

Title: _____

Title: _____

Date: _____

Date: _____

WVSTO Exhibit D

Work-In-Progress
Report Template

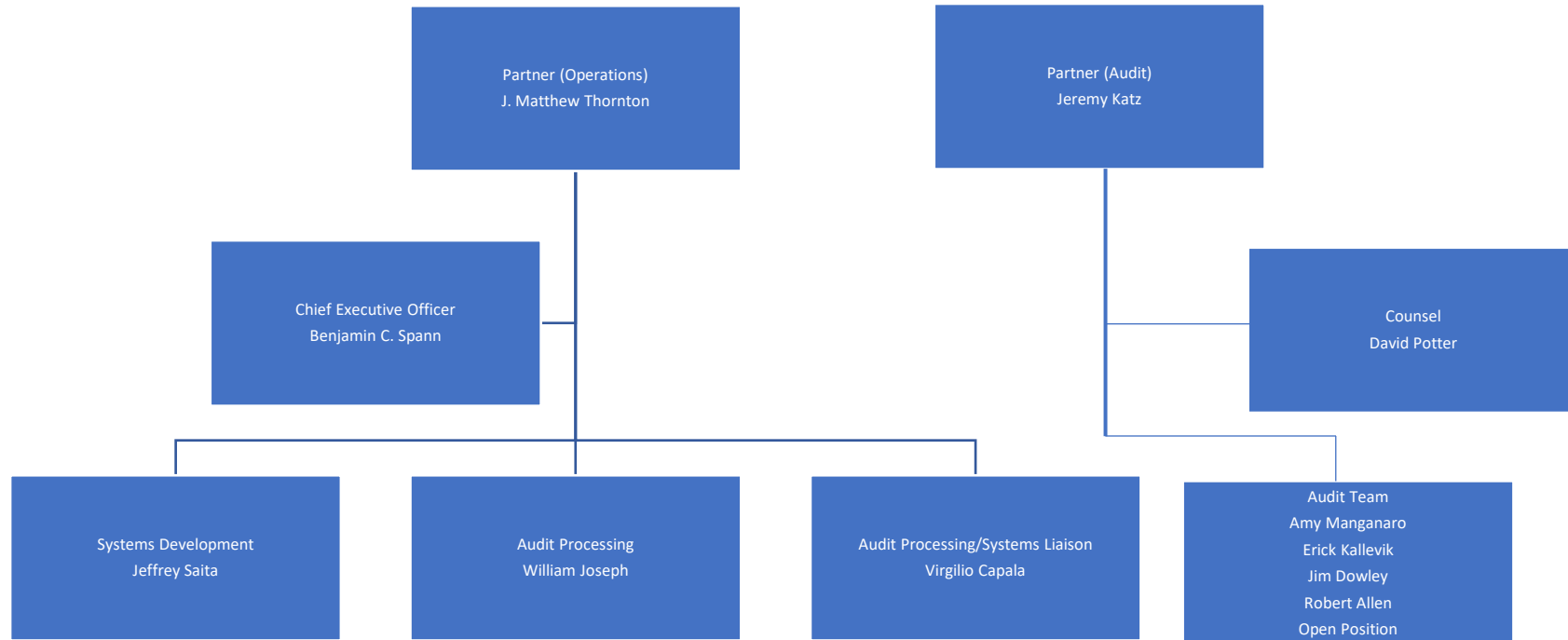
Exhibit D

[illegible]

ASUS EXHIBIT A

ASUS Organizational Chart

Audit Services US, LLC Organizational Chart



ASUS EXHIBIT B

Audit
Program

ASUS

AUDIT SERVICES, U.S., LLC

Audit Program

AUDIT INFORMATION SHEET

HOLDER: **«Company»**

ADDRESS: «Address1»

 «Address2»

 «City», «State» «PostalCode»

CONTACT: «FirstName» «LastName», «JobTitle»

TELEPHONE #: «WorkPhone»

FAX #: «Fax»

E-MAIL: «Email»

AUDIT DATE: _____

AIC _____

AUDITOR _____

AUDITOR _____

AUDITOR _____

WORKING PAPER INDEX
AUDIT PROGRAM
UNCLAIMED PROPERTY AUDIT

«Company»

Audit Cutoff date: _____

SECTION

CONTENTS

100	Report Guide Sheet, Manager Review
200	Audit Report
300	Telephone Record, E-mail, Faxes, and Correspondence
400	Audit Roster, Time Reports
500	Review of Internal Control-Questionnaire & Modules
501	_____
502	_____
503	_____
504	_____
505	_____
600	Audit Program
700	Auditors Notes, PreAudit Questionnaire Response, Record Requests
800	Holder Information
900	Unclaimed Property Reports – Analysis and Tests
1000	General Ledger Review Program
1100	Outstanding Checks & Drafts
1200	Credit Balances
1300	_____
1400	_____
1500	_____
1600	_____
1700	_____
1800	_____
1900	_____

«Company»

REPORT GUIDE SHEET

AUDIT OBJECTIVES

- A. Determine whether the scope of work defined in the respective sections of the Audit Program have been performed and that any significant matters or problems noted have been properly considered and resolved.
- B. Determine whether adequate audit evidence has been obtained to provide a reasonable basis for the report of audit.

WORKING PAPER REVIEW

We have satisfied the objectives for field work by performing the applicable procedures.

Holder Name: «Company»

Audit Cut-Off Date: _____

Date Records Reviewed Through: _____

Audit Report Date: _____

Report Approval:	<u>*Signature</u>	<u>Name</u>	<u>Date</u>
Auditor-In-Charge	_____	_____	_____
Audit Manager:	_____	_____	_____
Other:	_____	_____	_____

AUDIT PERSONNEL

Auditor's Initial Key

<u>Initials</u>	<u>Name</u>
_____	_____
_____	_____
_____	_____
_____	_____

* The signature should be entered only after the reviewer is satisfied that all review comments have been cleared (including appropriate revisions of the working papers) and the audit documentation is complete.

«Company»

MANAGER REVIEW PROGRAM

	<u>YES</u>	<u>NO</u>	<u>N/A</u>	<u>WORKING PAPER REFERENCE</u>
1. Has a draft of the audit report been prepared in respect to:	_____	_____	_____	_____
(1) Scope - Report Letter?	_____	_____	_____	_____
(2) Statement of Exam Findings?	_____	_____	_____	_____
(3) Management Advisory Comments?	_____	_____	_____	_____
2. Have all unresolved legal questions or controversies been cleared by legal counsel?	_____	_____	_____	_____
3. Are all positions taken in the audit consistent with prior positions taken in similar audits?	_____	_____	_____	_____
4. Are the Auditor's conclusions and opinions clear?	_____	_____	_____	_____
5. Have tests been adequately designed and executed to support the conclusions and opinions expressed by the A-I-C?	_____	_____	_____	_____
6. Are all positions taken by the A-I-C properly supported in the Unclaimed Property Law, regulations or office policy?	_____	_____	_____	_____
7. Have all non-relevant and unnecessary working papers been removed from the working paper file?	_____	_____	_____	_____
8. Has the A-I-C completed all required standardized forms relating to the audit?	_____	_____	_____	_____
9. Has the holder proposed adjustments to the audit findings?	_____	_____	_____	_____
10. Has the A-I-C properly examined and agreed to the proposed adjustments?	_____	_____	_____	_____
11. Has the Report Guide Sheet been completed?	_____	_____	_____	_____

**REPORT OF UNCLAIMED
PROPERTY EXAMINATION**

OF

«City», «State»

«Fein_»

**FOR THE REPORTING PERIOD
_____ THROUGH _____**

BY

AUDIT SERVICES, LLC

REPORT OF UNCLAIMED PROPERTY EXAMINATION

TABLE OF CONTENTS

DESCRIPTION	PAGE(S)
<i>EXAMINATION LETTER</i>	1
EXHIBIT A – Company Profile	2
EXHIBIT B – Limited Areas Examined	3-4
EXHIBIT C – Management Advisory Comment(s)	5
EXHIBIT D – Statement of Examination Findings	6

Audit Services
370 Lexington Avenue, Suite 707
New York, NY 10017

Telephone: (212) 594-5487
Facsimile: (212) 595-5571

August 11, 2022

Addressee

Dear _____:

In accordance with our engagement, we have performed the procedures described elsewhere in this report to the records discovered and provided by «Company» on behalf of the _____. The purpose of our examination was to determine the extent of compliance by «Company» with the unclaimed property laws of _____ and to identify, collect and deliver amounts due to the _____. The amounts identified as reportable to the _____ are \$_____ (Page 6, Exhibit D).

The report covers compliance issues for the period _____ through _____. Our examination included tests of the accounting records and the application of agreed-upon procedures which are explained in detail in Exhibit B of this report. The results of these procedures were utilized in arriving at amounts due. This report is intended solely for the use of the _____ and should not be used by those who have not agreed to the procedures and taken responsibility for the sufficiency of the procedures for their purposes. This report should not be associated with the financial statements of any entity.

Respectfully submitted,

Audit Services, US

«Company»

COMPANY PROFILE

«Company»

LIMITED AREAS EXAMINED

Our examination was designed to provide an analysis of the «Company»'s compliance with the related States' Unclaimed Property Laws. It involved interviewing with «Company» personnel, reviewing of the «Company»'s unclaimed property reports and examining specific records and documents. The following is a review of procedures applied.

Internal Control

We evaluated the system of internal control over property that becomes reportable under the Unclaimed Property Statutes of represented States by interviewing personnel familiar with the accounting procedures. Additionally, we requested a copy of the Company's manual relating to unclaimed property. According to Company personnel, no documented procedures or manual existed and none was provided. Based upon our evaluation of the Company's internal control we planned our examination accordingly. We found internal control weaknesses in the accounting and reporting of _____ that were presumed abandoned.

Disbursement Accounts

Bank statements and the related reconciliation were requested for _____ vendor checks. Our examination included reviewing for checks listed outstanding past the related dormancy periods and checks issued and subsequently voided or stopped payment.

We reviewed the general journal entries dated _____ to identify _____ checks that were credited to an income or expense account.

We further determined if these items had been reported to the respective States.

Accounts Receivable Credit Balances

We requested the accounts receivable aging for the examination period to review for customer credit balances and to determine if the Company was submitting the credit balances for lost accounts. Our review included tracing customer credit balances meeting the various States' dormancy period to the related unclaimed funds report. If the accounts receivable aging was unavailable we requested a list of customers with credit balances and determined if the Company was escheating the amounts.

We reviewed the general journal entries to identify accounts receivable credit balance items that were credited to an income or expense account.

Accounts Payable

We requested and analyzed accounts payable trial balances for lost vendors. Our review included examining the status on amounts due past the related dormancy periods where the Company had ceased doing business with the vendor. Any amounts identified were traced to the related States' report for proper reporting. If the accounts payable aging was unavailable, we requested a list of vendors placed on a "hold" status and reviewed for proper treatment.

General Ledger Detail and Subsidiary Ledgers

We requested and reviewed the chart of accounts and general ledger trial balances to select specific accounts to examine the detail for improper charge-off of escheat property and to identify accounts where unclaimed funds are generated and posted. Subsidiary Ledgers were requested for liability accounts containing escheat property and traced to the various States' unclaimed property reports.

Debt, Equity, Shares and Dividends

We requested information and schedules from the Company regarding debt and equity.

Employee Benefit Accounts

Employee benefit and retirement funds were requested to determine amounts due lost participants.

Additional Procedures

Additional records and documents were requested from the Company depending on the nature of its operations. The records and documents requested were transactions that lend themselves to produce abandoned property specific to their industry.

«Company»

MANAGEMENT ADVISORY COMMENT

Condition:

Requirement:

Recommendation:

We have concluded that the Company has not established adequate policies and procedures for assuring proper accounting and reporting of abandoned property. As a result of our examination the Company remitted all unclaimed property consisting of Expense Checks, Dividend Checks and Vendor/Supplier Checks. We are awaiting additional reports from the Company's transfer agent related to unclaimed dividends and the underlying shares. The Company has cooperated in this examination thus far and has agreed to cooperate in its completion. The Company has agreed to remit all escheatable property types discovered during our examination. Escheat amounts due are scheduled and listed in Exhibit D (Statement of Examination Findings) of this report.

The Company has been advised of its obligation to continue to report its abandoned and unclaimed property to the respective states as required by their respective unclaimed funds law.

«Company»

STATEMENT OF EXAMINATION FINDINGS
FOR THE PERIOD _____ THROUGH _____

<u>Description</u>	<u>Amount*</u> <u>Demandable</u>	<u>Amount**</u> <u>Reportable</u>	<u>Total</u> <u>Amount</u>
--------------------	-------------------------------------	--------------------------------------	-------------------------------

Total Findings

* Amount Demandable: This amount includes items which are past due according to the holding periods of the States we represent. The property should have been reported and remitted to the States in prior years.

** Amount Reportable: This amount includes items which should be reportable and remitted to the States we represent in the next year.

CORRESPONDENCE AND TELEPHONE RECORD

<u>INDEX OF CONTENTS</u>	<u>WORKING PAPER REFERENCE</u>
1) TELEPHONE CALL RECORD	301
2) _____	_____
3) _____	_____
4) _____	_____
5) _____	_____
6) _____	_____
7) _____	_____
8) _____	_____
9) _____	_____
10) _____	_____
11) _____	_____
12) _____	_____
13) _____	_____
14) _____	_____
15) _____	_____
16) _____	_____
17) _____	_____
18) _____	_____
19) _____	_____
20) _____	_____
21) _____	_____
22) _____	_____

Remarks: _____

«Company»

301.01

Spoke to: _____
(Name and Title)

Telephone # () _____ Date Called: _____ Auditor-Initials: _____

Remarks: _____

Spoke to: _____
(Name and Title)

Telephone # () _____ Date Called: _____ Auditor-Initials: _____

Remarks: _____

Spoke to: _____

Spoke to: _____ (Name and Title)

Telephone # () _____ Date Called: _____ Auditor-Initials: _____

Remarks: _____

«Company»

AUDIT ROSTER

	<u>Name & Title</u>	<u>Dept.</u>	<u>Phone</u>
1.	«FirstName» «LastName», «JobTitle»	_____	«WorkPhone»
2.	_____	_____	_____
3.	_____	_____	_____
4.	_____	_____	_____
5.	_____	_____	_____
6.	_____	_____	_____
7.	_____	_____	_____
8.	_____	_____	_____
9.	_____	_____	_____
10.	_____	_____	_____
11.	_____	_____	_____
12.	_____	_____	_____
13.	_____	_____	_____
14.	_____	_____	_____
15.	_____	_____	_____

«Company»

TIME ALLOCATION

AUDITOR:

[illegible]

«Company»
REVIEW OF INTERNAL CONTROL
GENERAL QUESTIONNAIRE

- | | <u>YES</u> | <u>NO</u> |
|---|------------|-----------|
| 1. Has the corporation ever changed its state of incorporation? If yes, obtain details. | _____ | _____ |
| 2. Has the holder reported unclaimed property in the past? | _____ | _____ |
| 3. Does the holder report unclaimed property to other states? W/P ref_____. | _____ | _____ |

*** IF 'NO' TO 2 AND 3 ABOVE DISREGARD THE FOLLOWING QUESTIONS**

- | | | |
|--|-------|-------|
| 4. Name of officer responsible for compliance with the Unclaimed Property Act. | | |
| _____ | | |
| 5. Name and title of person assigned to prepare the report: | | |
| _____ | | |
| 6. ARE REPORTS FILED:
Consolidated_____By Division_____ | | |
| 7. Are file copies and supporting documentation of reports maintained by the holder currently available? | _____ | _____ |
| If yes, | | |
| A. Where are they located?_____ | | |
| B. Who has custody?_____ | | |
| 8. Are reporting procedures or policies relating to unclaimed property documented in procedure or policy manuals? If yes, obtain a copy. | _____ | _____ |
| 9. What source does the holder use to determine its reporting responsibilities under the various states' laws? | | |
| _____ | | |
| _____ | | |
| _____ | | |
| 10. Does the holder use the criteria established in <u>Texas vs. New Jersey</u> when reporting to the states? | _____ | _____ |
| If no, what are the variances and reasons therefore? | | |
| _____ | | |
| _____ | | |
| _____ | | |
| Does the holder report no address property to its state of corporate domicile? | _____ | _____ |
| 11. If no, what is the disposition of such property? | | |
| 12. Does the holder consider any type of property exempt from the Unclaimed Property Act? | _____ | _____ |
| If yes, obtain details and legal position. | | |

«Company»

REVIEW OF INTERNAL CONTROL
GENERAL QUESTIONNAIRE (Con't)

	<u>YES</u>	<u>NO</u>
13. Is the holder relying on an opinion from legal counsel regarding its reporting responsibilities under the Unclaimed Property Act of state? If yes, obtain a copy. W/P Ref_____	_____	_____
14. Is the holder making any deductions or withholdings from any property that is subject to the Unclaimed Property Act on any State? If yes, obtain copies of the contract(s) authorizing the deductions. W/P Ref_____.	_____	_____
15. Has the holder been audited in the past? If yes, when? _____	_____	_____

«Company»

INTERNAL CONTROL QUESTIONNAIRE MODULE

 TYPE OF PROPERTY

- 1) Explain briefly how this type of property is accounted for and controlled:
(Prepare a transaction flowchart if required).

- 2) Is this type of property reported by the holder? Yes_____ No_____
If no, give reason:

- 3) Can the holder identify control and report this category of property? Yes_____ No_____
category of property?

- 4) INTERNAL CONTROL:
STRONG_____ ADEQUATE_____ INADEQUATE_____ WEAK_____

Date_____ Person
Interviewed_____ Auditor_____

Title _____

INTERNAL CONTROL QUESTIONNAIRE MODULE

TYPE OF PROPERTY

- 1) Explain briefly how this type of property is accounted for and controlled:
(Prepare a transaction flowchart if required).
- 2) Is this type of property reported by the holder? Yes_____ No_____
- If no, give reason:
- 3) Can the holder identify control and report this category of property? Yes_____ No_____
- 4) INTERNAL CONTROL:
STRONG_____ ADEQUATE_____ INADEQUATE_____ WEAK_____

Date_____ Person
Interviewed_____ Auditor_____

Title _____

«Company»

AUDIT PROGRAM

<u>INDEX</u>	<u>W/P REFERENCE</u>	<u>THIS APPLICATION</u>
		<u>YES</u>
I. OPENING THE EXAMINATION		
A. Pre-Audit Steps	601	X
B. Audit Opening	601	X
C. Audit Review	602	X
D. File Review	603	X
II. UNCLAIMED PROPERTY REPORT ANALYSIS	900	X
III. DETAILED EXAMINATION PROCEDURES BY CATEGORY		
1. Outstanding Checks & Drafts	1100	X
2. Credit Balances	1200	X
3. _____	_____	_____
4. _____	_____	_____
5. _____	_____	_____
6. _____	_____	_____
7. _____	_____	_____
8. _____	_____	_____
9. _____	_____	_____
10. _____	_____	_____

«Company»

(A) PRE-AUDIT STEPS

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Research the operations and history of the company.	_____	_____	_____
2. Obtain and review holder's correspondence to the States.	_____	_____	300
3. Obtain and review prior working papers, findings, if any from the States.	_____	_____	_____
4. Obtain and analyze copies of Annual Unclaimed Property Reports previously filed to the States.	_____	_____	900
5. Review responses to the Pre-Audit Request and prepare additional request as deemed appropriate.	_____	_____	_____
6. Schedule by phone or letter an agreeable time to begin audit.	_____	_____	300
7. Send an engagement letter confirming audit date along with records needed to conduct the examination.	_____	_____	_____
8. Assemble working paper file.	_____	_____	N/A

(B) AUDIT OPENING

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Advise the holder of the scope of the audit and relevant sections of the Unclaimed Property Law.	_____	_____	_____
2. Advise the holder of Audit Services's responsibilities under State agreements and audit guidelines.	_____	_____	_____
3. Obtain a general understanding of the accounting system and internal controls relating to unclaimed property.	_____	_____	_____
4. Inquire about the findings of internal and external auditors.	_____	_____	_____

«Company»

(C) AUDIT REVIEW

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Has the Internal Control Questionnaire been completed?	_____	_____	500
2. Has the Audit Program been completed?	_____	_____	100
3. Has the Audit Program been expanded as needed?	_____	_____	600
4. Were record retention schedules reviewed?	_____	_____	_____
5. Have holders' policy and procedures manuals been reviewed?	_____	_____	_____
6. Have financial statements been obtained?	_____	_____	_____
7. Advise holder of reporting requirements. This includes reporting forms, due dates, dormancy periods, etc.	_____	_____	_____
8. Hold the exit conference, fully discuss the findings and present appropriate working papers. ATTENDEES: _____ _____ COMMENTS: _____ _____ _____ _____	_____	_____	_____
9. Provide the holder _____ days to review the findings and propose adjustments. DATE TO RESPOND: _____	_____	_____	_____
10. Prepare a final Report and a Statement of Examination Findings and send to the holder.	_____	_____	200

«Company»

(D) FILE REVIEW

	<u>Yes</u>	<u>No</u>	<u>N/A</u>	<u>Reference</u>
1. Can the Statement of Examination Findings be traced to lead schedules?	_____	_____	_____	_____
2. Can the lead schedules be traced to the supporting documents?	_____	_____	_____	_____
3. Is the source of data clearly identified in the working papers?	_____	_____	_____	_____
4. Do all work papers (including attachments) reflect the holder name and other applicable information?	_____	_____	_____	_____
5. Were all records necessary to complete the audit available?	_____	_____	_____	_____
If not, was the ultimate disposition of non-available records resolved?	_____	_____	_____	_____
6. Were record storage areas searched by the auditors?	_____	_____	_____	_____
7. Have all open points been cleared?	_____	_____	_____	_____
8. Has the audit findings by State been completed or submitted to the processing center for processing?	_____	_____	_____	_____
9. Have all review notes been resolved?	_____	_____	_____	_____
10. File report. Date filed _____				

AUDITOR'S NOTES

[illegible]

*NUMBER, INITIAL AND DATE EACH NOTE PREPARED AND CROSS
REFERENCE TO THE APPROPRIATE WORKING PAPER REFERENCE.

«Company»

OUTSTANDING ISSUES

	<u>Outstanding Issue</u>	<u>Date of Last Contact</u>	<u>Date Resolved</u>	<u>Work Paper Reference</u>
1.	_____	_____	_____	_____
2.	_____	_____	_____	_____
3.	_____	_____	_____	_____
4.	_____	_____	_____	_____
5.	_____	_____	_____	_____
6.	_____	_____	_____	_____
7.	_____	_____	_____	_____
8.	_____	_____	_____	_____
9.	_____	_____	_____	_____
10.	_____	_____	_____	_____
11.	_____	_____	_____	_____
12.	_____	_____	_____	_____
13.	_____	_____	_____	_____
14.	_____	_____	_____	_____
15.	_____	_____	_____	_____

«Company»

RECORD(S) REQUEST

To: _____

Date: _____

From: _____

Needed By: _____

Records Requested:

_____ Holder located records requested.

_____ Holder could not locate records requested.

_____ Holder did not search for records requested.

The _____ has the authority to examine the records of any person with respect to holding, reporting, paying or delivering property that is subject to State(s) unclaimed property. Where records are not available or have been destroyed, it is permissible to estimate the holder's liability to the State(s) based upon the current information available from the holder.

Due to records not located or record areas not searched, an estimate will be performed as follows:

The above information has been presented and explained to me on _____

Signature

Authorized Official

Title

Date

«Company»

HOLDER INFORMATION

<u>TABLE OF CONTENTS</u>	<u>WORKING PAPER REFERENCE</u>
1) _____	_____
2) _____	_____
3) _____	_____
4) _____	_____
5) _____	_____
6) _____	_____
7) _____	_____
8) _____	_____
9) _____	_____
10) _____	_____
11) _____	_____
12) _____	_____
13) _____	_____
14) _____	_____
15) _____	_____
16) _____	_____
17) _____	_____
18) _____	_____
19) _____	_____
20) _____	_____
21) _____	_____

UNCLAIMED PROPERTY REPORT ANALYSIS

FIN: _____

DATE OF ESTABLISHMENT OR INCORPORATION: _____

STATE OF INCORPORATION:_____

LOCATION: _____

NUMBER OF EMPLOYEES: _____

REPORTING HISTORY (List oldest receipt first)

[illegible]

☐ IF HOLDER HAS NEVER FILED A POSITIVE REPORT TO THE STATE(S) , NO FURTHER TESTING IS REQUIRED IN THIS AREA.

REPORTING HISTORY REVIEWED BY:_____DATE:_____

COMMENTS: _____

«Company»

UNCLAIMED PROPERTY REPORT ANALYSIS

SOURCE: _____

PURPOSE: To determine if Reports of Unclaimed Property are properly completed in accordance with State Unclaimed Property Laws.

OPINION: _____

Audit Findings: YES _____ NO _____ W/P Ref. _____

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Prepare an analysis of reports previously filed.	_____	_____	900
2. Determine the states to which the holder files reports.	_____	_____	902
3. Review the holders files and related working papers used to prepare past reports to the state.			
(a) Examine previously filed unclaimed property reports and back-up information for completeness and accuracy.	_____	_____	_____
(b) Agree the owner names, addresses and amounts on unclaimed property reports directly to holder records.	_____	_____	_____
(c) Determine if statutory reductions taken are lawful.	_____	_____	_____
(d) Determine if any service charges have been applied against unclaimed property or if any property has been charged off completely. If service charges are			

taken report such to auditor
completing the affected section. _____

«Company»

UNCLAIMED PROPERTY REPORT ANALYSIS(CON'T)

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
4. Test dates of last transaction or dates property became payable, demandable, returnable or redeemable.	_____	_____	_____
5. Test for compliance with <u>Texas vs. New Jersey</u> rules.	_____	_____	_____
6. Test for compliance with the aggregation limit. (Amounts less than \$50.00)	_____	_____	_____
7. Determine if holder sends notices to owners prior to reporting funds.	_____	_____	_____
8. Recommendations (Acct. procedures, procedures for reporting to the state, and system inadequacies.)	_____	_____	_____

STATES FILED TO BY «Company»

<u>STATE</u>	<u>YES</u>	<u>YEAR FIRST REPORT FILED</u>
ALABAMA		
ALASKA		
ARIZONA		
ARKANSAS		
CALIFORNIA		
COLORADO		
CONNECTICUT		
DELAWARE		
DISTRICT OF COLUMBIA		
FLORIDA		
GEORGIA		
GUAM		
HAWAII		
IDAHO		
ILLINOIS		
INDIANA		
IOWA		
KANSAS		
KENTUCKY		
LOUISIANA		
MAINE		
MARYLAND		
MASSACHUSETTS		
MICHIGAN		
MINNESOTA		
MISSISSIPPI		
MISSOURI		
MONTANA		
NEBRASKA		
NEVADA		
NEW HAMPSHIRE		
NEW JERSEY		
NEW MEXICO		
NEW YORK		
NORTH CAROLINA		
NORTH DAKOTA		
OHIO		
OKLAHOMA		
OREGON		
PENNSYLVANIA		
PUERTO RICO		
RHODE ISLAND		
SOUTH CAROLINA		
SOUTH DAKOTA		
TENNESSEE		
TEXAS		
UTAH		
VERMONT		
VIRGIN ISLANDS		
VIRGINIA		
WASHINGTON		
WEST VIRGINIA		
WISCONSIN		
WYOMING		

GENERAL LEDGER REVIEW

	REF.
1. Chart of Accounts	1001
2. Document General Ledger Accounts reviewed as deemed necessary:	
Possible accounts to be reviewed:	
Miscellaneous/Other Income	
Write Off Accounts	
Suspense Accounts	
Stale dated/Dormant Accounts	
Adjustment/Offset Accounts	
3. Review Journal Entries as deemed necessary:	

«Company»

OUTSTANDING CHECKS & DRAFTS
Two Party Instruments

SOURCE: _____

PURPOSE: To determine if outstanding checks that are deemed unclaimed are reported in accordance with the Unclaimed Property Laws.

OPINION: _____

Audit Findings: Yes _____ No _____ W/P Ref. _____

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Obtain a list of all open and closed bank accounts.	_____	_____	_____
2. Obtain a copy of the latest bank reconciliations for all disbursement accounts:	_____	_____	_____
a. Agree balances to the general ledger (GL) and the bank statement (A).	_____	_____	_____
b. Trace total outstanding checks to the bank reconciliations(T).	_____	_____	_____
c. Age and schedule outstanding checks through audit cut-off date.	_____	_____	_____
3. Review the last bank reconciliation for all closed disbursement checking accounts prior to closing.	_____	_____	_____
a. Trace total outstanding checks to the bank reconciliation.	_____	_____	_____
b. Determine disposition of outstanding checks when account was closed.	_____	_____	_____
c. Age and schedule outstanding checks as deemed necessary.	_____	_____	_____

«Company»

OUTSTANDING CHECKS & DRAFTS
Two Party Instruments

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
4. Review liability accounts to which outstanding checks are transferred:			
a. Test debit entries to determine their nature.	_____	_____	_____
b. Age and schedule outstanding checks as deemed necessary.	_____	_____	_____
5. Analyze selected accounts to determine whether any outstanding checks have been written-off or reversed. (See 1000 for possible accounts to review.)	_____	_____	_____
a. Age and schedule outstanding checks as necessary.	_____	_____	_____
6. Document holder's check voiding policy.	_____	_____	_____
a. Test a sample of voided checks.	_____	_____	_____
7. Document how "Returned by Post Office checks are handled.	_____	_____	_____
8. Document the availability of names and last known addresses of owners of unclaimed property.	_____	_____	_____
9. Recommendations (Acct. procedures, procedures for reporting to the state, and system inadequacies.)	_____	_____	_____

«Company»

CREDIT BALANCES

Accounts Receivables, Payables, Etc.

SOURCE: _____

PURPOSE: To determine if credit balances that are deemed unclaimed are reported in accordance with the Unclaimed Property Laws.

OPINION: _____

Audit Findings: Yes _____ No _____ W/P Ref. _____

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Obtain a list of all categories of credit balances generated by the holder.	_____	_____	_____
2. Review a listing of credit balances to:			
a. Evaluate aging procedures. Date of oldest credit should be documented.	_____	_____	_____
b. Test debit entries to determine their nature.	_____	_____	_____
c. Schedule credit balances held past the statutory time period and reportable as deemed necessary.	_____	_____	_____
3. Document holders policy for handling small credit balances.	_____	_____	_____
4. Analyze income accounts to determine whether credit balances have been taken into income.	_____	_____	_____
5. Review related expense accounts to determine whether credit balances are used to offset expenses.	_____	_____	_____
6. Schedule credit balances written off.	_____	_____	_____
7. Document availability of names and last known addresses of owners of unclaimed property.	_____	_____	_____
8. Recommendations (Acct. procedures, procedures for reporting to the state, and system inadequacies).	_____	_____	_____

«Company»

Stock, Dividends, Underlying & UNDELIVERABLE Shares,

Bond Principal & Interest

SOURCE:

PURPOSE: To determine if stock, dividends, underlying shares, undeliverable shares, Bond principal & interest deemed unclaimed are reported in accordance with the Unclaimed Property Laws.

OPINION:

Audit Findings: YES _____ NO _____ W/P REF. _____

I. Preliminary Examination Steps:

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
1. Research outside sources such as Capital Changes Reports prior to commencing the examination. Analyze the history of the holder, i.e., classes of stock outstanding, stock splits, stock dividends, mergers, acquisitions, spin-offs, etc.	_____	_____	_____
2. If the company uses an outside transfer agent submit a records request to the company and have them request the records identifying unexchanged and/or undeliverable stock certificates.	_____	_____	_____
3. Obtain a list of matured or called debt (bonds, debentures or notes) for the holder and/or merged companies.	_____	_____	_____

II. MergersN/A ☐

1. Evaluate and document the systems and procedures and internal controls used to report this property.
 - a) Request a copy of written procedures if available.

_____	_____	_____
_____	_____	_____

2. Prepare a list of all merged or acquired companies.

a) Obtain agency contracts relating to applicable mergers, acquisitions, and liquidations.

b) Determine if the merged company filed reports with the state. Obtain and review copies of these reports for any previously reported property.

c) If applicable, for each merger send a records request to the transfer agent and complete the required stock/dividend worksheets

III. Stocks – Underlying & Undeliverable

N/A ☐

1. Evaluate and document the systems, procedures and internal controls used to identify and report this property. (61-1)

a. Request a copy of written procedures if available.

2. Obtain any legal opinions relating to the reporting of stock dividends, underlying shares, etc.

3. Determine if authorizations have been given by the holder to the agent to report unclaimed property to selected states.

4. Evaluate and document the carry-forward of potential unclaimed property from **prior** transfer or paying agents and the ultimate disposition of same.

5. Reconstruct charges on any items or items charged-off completely.

6. Trace items previously reported to the state to source records and note any exceptions.

7. Prepare a schedule(s) of shares held in excess of the statutory holding period.

IV. Cash and Stock Dividends

N/A ☐

1. Evaluate and document the systems, procedures and internal controls used to identify and report this property. _____
2. Obtain or construct a five year dividend and cash-in-lieu of fractions payment history. (i.e., dates paid and dollar amounts per share) _____
3. Request a printout or schedule of outstanding dividend checks by payee. It may be necessary to have the company contact their paying agent for these records. _____
 - a) Review outstanding dividend check and cash-in-lieu of fractions history and identify those payees with five year history of non-negotiated checks. _____
 - b) List the shares belonging to these payees as potentially reportable shares. _____
 - c) List outstanding dividends and cash-in-lieu paid on these shares, through the current period as potentially reportable. (63-1) _____

V. Principal and Interest on Debt Issues

N/A ☐

1. Evaluate and document the systems, procedures and internal controls used to identify and report this property. _____
2. Review the long-term liabilities section of the general ledger. Identify and record current bond issues outstanding. Discuss the outstanding issues with relevant personnel to determine if any calls or serial maturities have taken place during the audit. Request a list of bond issues for which the trust department is paying agent and which have begun serial redemption or have had calls. _____

	<u>Initial</u>	<u>Date</u>	<u>Reference</u>
3. If the company uses an outside agent submit a records request to the company and have them request the records identifying bond and interest transactions.	_____	_____	_____
4. If the company is its own paying agent, review a current reconciliation and balance unpaid items to control totals.	_____	_____	_____
5. Account for debt redemption's, calls, maturities, and the disbursement of interest payments for registered and bearer debt instruments. (Until the early 1960's, most debt securities were issued in bearer form.)	_____	_____	_____
6. Review pertinent sections of the bond or debenture indenture agreements requiring the trustee to:			
a) Return outstanding and undeliverable interest checks or proceeds from unresented coupons or uncashed checks to the holder after a stipulated period of time.	_____	_____	_____
b) Registration requirements of the security by the issuer of the owner.	_____	_____	_____
7. Review currently open and closed principal and interest control accounts for:			
a) Unreported property.	_____	_____	_____
b) Property service charged or charged off.	_____	_____	_____
8. Prepare a schedule of all principal and interest held in excess of the statutory holding period.	_____	_____	_____

ASUS EXHIBIT C

Audit
Operating
Procedures
Manual

ASUS

AUDIT SERVICES, U.S., LLC

Audit Operating Procedures Manual

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

AUDIT SERVICES U.S., LLC PROCEDURES MANUAL INDEX

<u>Procedure</u>	<u>Procedure Number</u>
<u>Planning the Audit</u>	
Professional Conduct	2018-02
Training of Unclaimed Property Auditors	2018-04
Holder Research	2018-06
Reporting History	2018-08
Selecting Audit Candidates	2018-10
Selecting Candidates for Involuntary Audits	2018-12
Contact with Holders	2018-14
Scheduling Examinations	2018-16
Pre-entrance Request	2018-18
<u>Conducting the Audit</u>	
General Audit Standards	2018-20
Use of Audit Programs	2018-22
Audit File Format	2018-24
No Date Property	2018-26
No Address Property	2018-28
Underlying Shares and the Determination of Abandonment	2018-30
Bankruptcies	2018-32
Out of Proof Reports	2018-33
Locating and Evaluating Historical Records	2018-34
Estimates	2018-36
Auditing for Multiple States	2018-38
Work paper Technique	2018-40
Documentation Requirements	2018-42
Demandable, Reportable and Reinstatable Property	2018-44
Problem Holders	2018-46
Concurrent Audits - Conflicts & Resolution	2018-48
<u>Audit Results</u>	
Audit Report	2018-50
Amended Findings	2018-52
Audit Review	2018-54
Follow-up on Audit Findings	2018-55
Remittance of Property from Holder	2018-56
Submission of Data by Holder	2018-57
Final Reconciliation of Audit Findings	2018-58

<u>Audit Results (Cont)</u>	<u>Procedure Number</u>
------------------------------------	--------------------------------

Process Unclaimed Property Data	2018-59
Report and Remit Unclaimed Property	2018-60
Follow-up when no Report Received	2018-61
Audit Protest	2018-64
Filing and Maintenance of Audit Files	2018-66

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: 2018-02

Effective Date: January 1, 2018

Approval: _____

SUBJECT: PROFESSIONAL CONDUCT

PURPOSE: To ensure high standards of performance for the Unclaimed Property audit staff.

DISCUSSION: Professional conduct provides holders and co-workers a basis for confidence in the abilities and competence of the auditors. Auditors are to perform all responsibilities in a professional manner both in and out of the office.

PROCEDURE: I. GENERAL STANDARDS OF CONDUCT

- A. Members of the audit section must conduct themselves in a professional manner, and are to dress accordingly. In order to project a professional image, auditors should be punctual, tactful, and courteous to co-workers and holder personnel.
- B. Auditors are to have knowledge of the Unclaimed Property Law and are to operate within the law.
- C. Unclaimed Property Auditors are to display a professional attitude toward work.
- D. Unclaimed Property Auditors must remember we are agents of the states that we represent

II. PROFESSIONAL CONDUCT AT THE AUDIT SITE

- A. During an examination, auditors will adhere to the policies and procedures of the holder. Auditors should generally work the same hours as the holder.
- B. Client records are to be handled carefully. If records are provided by holder personnel, return the records when they are no longer needed. Records removed from the holder's files by Unclaimed Property Auditors are to be properly re-filed.
- C. The Unclaimed Property Auditor is to hold in strict confidence all information concerning the holder's affairs that is acquired during the course of the audit. The auditor must adhere to the conditions of the Confidentiality Agreement with the holder.

III. COMMUNICATION WITH HOLDERS

- A. When speaking to holder personnel, communications should pertain to business only. Limit discussions to the audit subject matter. If discussion of a personal nature is initiated by the holder, respond courteously, and then return the conversation to the business at hand.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 2

Procedure Number: 2018-02

- B. Be attentive to holder inquiries, and provide sufficient information to assist the holder in understanding the Unclaimed Property Laws of each State represented.
- C. When presenting the audit findings to the holder during the closing conference, disclose all information that may assist the holder in understanding the findings. Auditors must be knowledgeable of Unclaimed Property laws in order to provide a reasonable basis for the audit findings.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number:: 2018-04

Effective Date: January 1, 2018

Approval: _____

SUBJECT: TRAINING OF UNCLAIMED PROPERTY AUDITORS

PURPOSE: To describe the procedures used for training of new and existing unclaimed property auditors.

DISCUSSION: The goals and objectives of Audit Services, U.S., LLC can only be reached by skilled personnel. The training of auditors is a continuous process and must be given priority.

PROCEDURE: I. TRAINING PROCEDURES

A. Provide in-house training

All staff members should be given in-house training to familiarize them with the basics of the unclaimed property program.

B. Provide on-the-job training

All staff members should be given ample opportunity to apply the principles and techniques of the audit program to gain more experience, proficiency and confidence in work performance.

C. Periodic evaluation of work performance

This is helpful in determining the level of competence achieved by an individual staff member. In addition, it can be determined if special attention is needed to put more effort in any particular area for comprehensive training.

D. Professional Materials

Staff is encouraged to read materials in order to stay abreast of new methods and techniques in area of expertise and developments involving unclaimed property matters.

E. Continuing education, seminars and workshops

This will keep an employee well-informed about new developments in the field.

F. Specialization

The training program should provide for the selection of such auditors who could be given training in a specialized area for which the auditor is most suited.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

Procedure Number: 2018-04

SUBJECT: TRAINING OF UNCLAIMED PROPERTY AUDITORS

G. Types of staff training programs

- Outside consultants
- Inside workshops
- Seminars and courses offered by State and Federal government
- Individual initiative to pursue additional course study

II. CROSS TRAINING

- A. Final aspect of the training program is to provide cross training of staff members at various levels within Audit Services.

III. RESOURCES

- A. Unclaimed Property Statutes from States
- B. ASUS Audit training manual
- C. Audit procedures
- D. Guide to Unclaimed Property and Escheat Laws by Anthony Andreoli, CPA
- E. Unclaimed Property Law and Reporting Forms by David Epstein
- F. Related accounting and law books
- G. Courses and reference material related to computer programs that assist in analyzing records and documenting the audit work performed.

IV. EVALUATION TECHNIQUES

- A. Review notes by Auditor-in Charge
- B. Review notes by Director of Audits
- C. Performance Review

V. TRAINING TIMETABLE

- A. During the probationary period, new auditors will be evaluated six months from employment date to determine if performance is satisfactory and if employment should be continued.

- B. The attached “Skills to Develop During Training” will enable new auditors to know what is expected of them.

**SKILLS TO DEVELOP
DURING THE FIRST
EIGHT WEEKS OF TRAINING**

The Auditor should:

1. Understand the concepts of Unclaimed Property Law.
2. Understand the format of the work paper binder.
3. Be knowledgeable of the sections in the Audit file and the purpose of each step.
4. Be able to follow the audit program and know the purpose of each step.
5. Be able to document systems involved in the audit (i.e. questionnaires, narrative, or flowchart).
6. Be able to number work papers and understand how to cross reference all work.
7. Know the sections of the Unclaimed Property Statutes and court cases that are relative to the audits she/he has worked.
8. Be able to prepare and organize work papers for specific tests in logical sequence.
9. Be able to write certain sections of the audit report, (i.e. Statement of Examination Findings, Letter to the holder, Management Advisory Comments, and supporting schedules)
10. Be able to complete certain tests relative to the audits.
11. Understand the terms, “demandable, reportable, and reinstatable” and be able to schedule accordingly.
12. Read all materials assigned in training sessions.
13. Be familiar with operations of Audit Services.
14. Be able to research Holder’s history.
15. Become familiar with use of computers and programs (Audit Selector, APRS & Hoovers).
16. Be able to assist others in all areas of the audit.
17. Be able to prepare a monthly time report.

SECOND EIGHT WEEKS OF TRAINING

The Auditor should:

1. Be able to conduct interviews with holder's personnel to ascertain pertinent information to document the systems.
2. Know the sections of the Unclaimed Property Law relevant to the audit.
3. Be able to carry figures forward from supporting work papers, to Schedule of Examination Findings and to Statement of Examination Findings.
4. Know how to write the complete Audit Report.
5. Know states in which we have contract and states that do not have laws covering certain property.
6. Be able to respond to holder's questions and support response by referencing section of the law. Know when to refer such questions to Auditor-in-Charge or Director of Audits for guidance.
7. Be able to handle telephone inquiries regarding unclaimed property.
8. Be able to conduct holder contacts.

THIRD EIGHT WEEKS OF TRAINING

The Auditor should:

1. Be able to select, schedule, and conduct an examination as an Auditor-in-Charge.
2. Know how to review a completed examination.
3. Understand the entire audit process and be able to assist in training new auditors.
4. Be able to reference the Unclaimed Property court cases as they apply to situations that arise during the audits. Know how to apply issues and subject matter to factual situations.
5. Be able to present audit findings to holders.

AUDIT SERVICES, U. S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: 2018-06

Effective Date: January 1, 2018

Approval: _____

SUBJECT: HOLDER RESEARCH

PURPOSE: To describe the procedures used to ensure that holders report and remit all types of unclaimed property belonging to residents of the States.

DISCUSSION: When the States authorize enforcement of the unclaimed property statutes to be accomplished through field audits. Research consists of reviewing and reacting to deficiencies in Unclaimed Property reports and researching and corresponding with holders not presently on the States' holder database.

PROCEDURE: I. SELECTING HOLDERS FOR RESEARCH

A. Auditor selects holders for research through the following sources:

- (1) State requests
- (2) Business Magazines and Newspapers
- (3) Audit Selector
- (4) Annual financial reports of companies
- (5) Holder cooperative compliance
- (6) Personal experience or contact
- (7) Transfer Agent Client Roster
- (8) Securities Industry Experience

B. Auditor researches holder on the audit selector database for the following:

- (1) Reporting history of unclaimed property
- (2) Subsidiaries-who files unclaimed property reports for them
- (3) Mergers and Acquisitions-date and type of activity
- (4) Physical location and company attributes

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: HOLDER RESEARCH

Procedure Number: 2018-06

- (5) Obtain an understanding of the holder's business activities in order to determine the possible unclaimed property reporting types that may be involved.

C. Sources used to determine the above:

- (1) Prior unclaimed property reports filed
- (2) Hoovers and the Internet
- (3) Commerce Clearing House/Capital Changes Reporter
- (4) Financial Stock Guide
- (5) Comparative Data Bases

II. ANALYZE REPORTS/POSITIVE & NEGATIVE

A. Auditor analyzes the reporting history for the following:

- (1) Omissions of property types
- (2) Only Negative reports being filed
- (3) Unauthorized deductions
- (4) No reports being filed
- (5) Errors with remittance

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: 2018-08
Effective Date: January 1, 2018
Approval: _____

SUBJECT: REPORTING HISTORY

PURPOSE: To describe procedures used in obtaining a reporting history of a holder.

DISCUSSION: Reporting history of a holder should be obtained before an engagement letter is mailed or examination performed. This information can be obtained from three sources: audit selector, the States, and the holder.

PROCEDURE: I. THE AUDIT SELECTOR

A. Reporting history for holders from historical to current can be viewed on The Audit Selector.

- (1) Holders can be identified on the audit selector by name, Tax ID, or Holder ID. Some holders may have multiple Holder ID's.
- (2) Review reporting history summary by year for selected Holder.
- (3) Review detailed reporting history by property type.
- (4) Audit Selector database may be sorted by SIC code, company name, location, asset size, number of employees, dollar amounts reported, assigned audits, and corporate structure.

II. STATE'S DATA BASE

State listings show the reporting history of a holder for the years the holder has reported and are listed by the holder number. Request a complete holder reporting history from each state represented in the audit.

III. HOLDER'S RECORDS

The holder usually has copies of all reports submitted to the States along with backup information. A records request should include all copies and backup information used to prepare the report.

IV. TRANSFER AGENT'S DATA BASE

The Transfer Agent listing provides potential holders who have had Mergers & Acquisitions or a Corporate Action event that may contain eligible escheatable property.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 3

Procedure Number: 2018-10

Effective Date: January 1, 2018

Approval: _____

SUBJECT: SELECTING AUDIT CANDIDATES

PURPOSE: To select for audit the holders who have the greatest potential of noncompliance.

DISCUSSION: The Unclaimed Property Laws provide that State Administrators may at reasonable times and upon reasonable notice examine the records of any person with respect to holding, reporting, paying or delivering any property that is required to be reported.

PROCEDURES: I. SOURCE OF SELECTION

A. State Requests

- a. Complaints from customers or citizens.
- b. Information derived from past contacts and audits.
- c. States can inform where they are finding noncompliance.
- d. Noncompliance in one State could mean noncompliance in other States.
- e. Experience with one holder in an industry may generate interest in other holders in the same industry.

B. Review of Audit Selector and/or annual unclaimed property reports and notes:

- (1) Did first report filed cover the entire reach back period permissible under the law?
- (2) Omissions of categories of property and/or information that the holder would be expected to file.
- (3) Disclosure of estimates rather than actual amounts.
- (4) No aggregate (amounts under \$50).
- (5) Disclosure of a deduction that does not contain a copy authorizing the deduction or citation of authority.
- (6) Non-reporting or negative reports.

C. Industry Analysis - Industry standards and measurements (if available) of a possible audit candidate are reviewed for comparison to that of other holders in the same industry.

D. Computer databases (i.e. Hoovers, Moody's, Dunn & Bradstreet, Google, Onesourceexpress, CCH, etc.).

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 3

SUBJECT: SELECTING AUDIT CANDIDATES

Procedure Number:

2018-10

- E. Newspaper, magazine articles, and other publications.
- F. Transfer Agent Roster - Information derived from past event dates, contacts and audits.

II. CONSIDERATIONS

- A. Geographic Location - The audit candidate should be in a location that makes the trip worthwhile as far as cost vs. potential benefits is concerned.
- B. Size of Company - A smaller company is less likely to have a large amount of unclaimed property. A contact would serve better.
- C. Report History - A company that is reporting properly, compared to similar companies is less likely to be a strong audit candidate.
- D. Type of Holder - Certain types of holders will be more practical to audit than others.
- E. Previous Audit - Review work paper file of the previous audit for a reporting pattern.
- F. Political - Recognize States' sensitivities toward holders operating within the State.

III. BACKGROUND INFORMATION

- A. Reporting history - Research records for each potential audit candidate and record all the past report files.
- B. Review and obtain any information relative to the potential audit candidate in the stock and dividend area. (i.e. Hoovers, Moody's)
- C. All States - Request and review all information submitted by the States.

IV. HOLDER'S ACCOUNTING TECHNIQUES

- A. Determine if the holder has a computer or accounting system that doesn't account for unclaimed property.
- B. Unclaimed Property is usually a low priority among most holders.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 3 OF 3

SUBJECT: SELECTING AUDIT CANDIDATES PROCEDURE NUMBER: 2018-10

- C. Holders with strong internal controls over potential unclaimed property reduce the probability of audit findings.

V. SELECTION PROCESS

- A. File of Audit Candidates - The audit unit utilizing the above-mentioned sources and considerations will identify possible audit candidates.
- B. Prioritize Candidates
 - (1) Audit 1- Companies identified through compliance work that are higher priority and need to be audited as soon as possible (within the year).
 - (2) Audit 2 – Companies identified through compliance work that are lower priority and should be audited in the future (within 3 years).
 - (3) Audit 3- Companies/Industries identified by States that need to be audited within a specified time period.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: 2018-12
Effective Date: January 1, 2018
Approval: _____

SUBJECT: SELECTING CANDIDATES FOR INVOLUNTARY AUDITS

PURPOSE: To select the holders who appear to have the greatest potential of noncompliance for involuntary audits.

DISCUSSION: The Unclaimed Property Laws state that the State Administrators may at reasonable times and upon reasonable notice examine the records of any person with respect to holding, reporting, paying or delivering any property that is required to be reported. Audit candidates may be selected by the States or from a list prepared by Audit Services, U.S., LLC

PROCEDURES: I. SOURCE OF SELECTION

- A. State Authorized Examination - State provides ASUS with the name of a potential audit along with reason to believe and reporting history.
- B. ASUS prepares list of audit candidates and presents to the States.
- C. Suggested guidelines to follow: Procedure 2018-10 "Selecting Audit Candidates".

II. EXAMINATION PROCESS

A. Lead State

States have the right to audit records of non-domiciliary for unclaimed property and States have the sovereign right to audit any holder; however, in order to be more efficient it may be practical for an audit to be called by:

- (1) The state of incorporation
- (2) The state of corporate headquarters
- (3) The state of principal place of business
- (4) A state where a division, branch or subsidiary is located
- (5) A state with a significant business presence
- (6) Any other reason to believe the company is holder property belonging to your state

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

Procedure Number: 2018-12

SUBJECT: SELECTING CANDIDATES FOR INVOLUNTARY AUDITS

- B. ASUS prepares and sends Background Information Package to states for approval. Package includes the following information:
 - (1) Corporate history, organization chart, financial statements, subsidiaries, divisions, etc.
 - (2) Where all record-keeping, accounting and unclaimed property reporting is performed.
 - (3) Record-keeping centralized or cost centers
 - (4) Third party administrators and paying agents
- C. States will do the following:
 - (1) Review Background Information Package
 - (2) Ensure no State or Vendor has, or is, auditing Holder
 - (3) Notify ASUS of audit approval
 - (4) Submit background information including holder's reporting history.
- D. After notification by states, ASUS will:
 - (1) Add State to list of represented States
 - (2) Verify holding periods and specific instructions from State
- E. The states formally notify the Holder of the audit and then ASUS contacts Holders and informs Notice of Intent to Examine on behalf of States by:
 - (1) Telephone conference with holder's contact person announcing audit intentions and request for basic information.
 - (2) Follow-up telephone conference setting date for examination to begin.
 - (3) Send entrance letter to holder with Documentation Request
 - (4) Place on Work in Progress Report

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-14**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: CONTACT WITH HOLDER

PURPOSE: To describe the procedures used for assisting the States in contacting holders concerning compliance with the Unclaimed Property Laws of the States.

DISCUSSION: It is necessary to contact holders who are not in compliance with the Unclaimed Property Law to stimulate compliance. Often a letter or telephone call is more efficient than a field audit.

PROCEDURE: I. WRITTEN CORRESPONDENCE

A. Correspond in writing to holders concerning the following:

- (1) Filing of reports (i.e. None or Negative).
- (2) Omission of property types relative to holder.
- (3) Holder is not listed on holder data base.
- (4) Any unreported property from mergers or acquisitions.
- (5) Any other reporting obligations.

II. TELEPHONE CONTACTS

- A. Contact holders via telephone when the situation does not necessitate a letter.
- B. Respond to inquiries from the holders concerning compliance with the Unclaimed Property Law.
- C. Record all telephone conversations on the Telephone Call Record or Auditor's Notes form and file these in the correspondence folder for the holder.

III. FOLLOW-UP TO HOLDER CONTACT

- A. Review all correspondence received as a result of a compliance letter.
- B. Respond to all correspondence. Place all correspondence in the holder compliance folder.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: CONTACT WITH HOLDER

Procedure Number: 2018-14

- C. Review all unclaimed property reports received as a result of holder contact and determine if they have been completed properly. Place a copy of the reports in the holder's compliance folder.
- D. Follow-up with the holder either by letter or telephone if the report is not completed properly.
- E. Submit the following to the Auditor:
 - (1) Holder's compliance file folder
 - (2) Compliance information sheet
 - (3) Monthly activity report information
- F. Auditor will update compliance control file on database and file holder's compliance folder.
- G. Recommend possible audits or contacts to the Director of Audits.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-16**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: SCHEDULING EXAMINATIONS

PURPOSE: To describe the procedures used to schedule.

DISCUSSION: In order to maximize productivity and to minimize the inconvenience to the holder, examinations are to be performed upon written notice to the holder and upon holder confirmation of an examination date.

PROCEDURE: I. SCHEDULING EXAMINATIONS

- A. Candidates are selected for audit based on set priorities (See Procedure "Selecting Audit Candidates" 2018-10).
- B. Telephone selected candidates announcing audit intentions and schedule mutually agreeable date (See Procedure "Pre-entrance Requests" 2018-18).
- C. An entrance letter confirming the examination starting date and requesting records is sent to each candidate (See Procedure "Pre-entrance Requests" 2018-18).
- D. Make reservations for travel and accommodations if needed.

II. CONFIRM EXAMINATION

- A. Approximately one week prior to audit, contact holder to confirm audit date and time and that the requested documentation is ready.
- B. Inquire as to any questions the holder may have.

III. RE-SCHEDULING EXAMINATIONS

- A. After entrance letter is sent, holder may contact AIC to reschedule the audit.
 - (1) Encourage holder to keep original date scheduled
 - (2) Reschedule audit as soon as possible.
 - (3) Send letter confirming the new audit date.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: Scheduling Examinations

Procedure Number:

2018-16

B. Holder may request to re-schedule audit a second time.

(1) Select rescheduled audit date.

(2) Send letter confirming both new audit date and that interest begins accruing if applicable.

IV. REFUSAL OF HOLDER TO SCHEDULE EXAMINATION

See Procedure "Problem Holders" 2018-46

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-18**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: PRE-ENTRANCE REQUEST

PURPOSE: To describe the procedures used to confirm an examination and request information.

DISCUSSION: Prior to examination, the Auditor-In-Charge notifies holder of date of examination by phone and follows-up with a letter confirming date and requesting information.

PROCEDURE: I. CONTACT PERSON VIA TELEPHONE TO:

- A. Explain briefly the audit program and areas that will be examined.
- B. Confirm date for examination to begin.
- C. Establish arrival time.
- D. Ask for directions to exam site.
- E. Request working hours.
- F. Ask if parking is available.
- G. Inquire as to nearby hotels.
- H. Inquire regarding work space availability.

II. SEND ENTRANCE LETTER (SEE ATTACHED)

- A. Context of letter should confirm the following:
 - (1) Date examination begins.
 - (2) Arrival time.
 - (3) Number of auditors
 - (4) States representing
- B. Request the related records including:
 - (1) Prior unclaimed property reports including supporting work papers.
 - (2) Internal memos or legal opinions relating to unclaimed property.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: PRE-ENTRANCE REQUEST

Procedure Number:

2018-18

- (3) Accounting and operational policies and procedures pertaining to unclaimed property.
- (4) Description of the holder's unclaimed property identification and reporting process and systems.
- (5) Records retention schedule.
- (6) Copy of the latest financial report including notes.
- (7) Descriptive Chart of Accounts.
- (8) Bank reconciliations and outstanding check listings for all active and closed disbursement accounts for the past five years along with their respective bank statements. The outstanding check lists should include check issue dates.
- (9) Written documentation of check voiding policy and how outstanding checks are cleared.
- (10) Detailed general ledger for the last month of the last fiscal year which includes closing and adjusting entries.
- (11) Detail of any general ledger accounts containing unclaimed property.
- (12) Aged accounts receivable credit balance reports, if applicable.
- (13) General journal entries for the past five years, including closing and adjusting entries.
- (14) Accounting procedures concerning unidentified remittances and detail of any account(s) containing unidentified remittances.
- (15) Listing of institutions acting as dividend or bond paying agents and/or stock transfer agents for the holder and its subsidiaries, if a publicly held company, note if more than one agent.
- (16) Names, addresses and contact information of third party administrators who do disbursements for the holder.
- (17) Policies and procedures regarding rebates and other payments to customers.
- (18) List of uncashed payroll and employee benefit payments.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 3

Procedure Number: 2018-20

Effective Date: January 1, 2018

Approval: _____

SUBJECT: GENERAL AUDIT STANDARDS

PURPOSE: To set forth audit standards for the performance of Unclaimed Property audits.

DISCUSSION: General auditing standards form the basis for the execution of the audit for unclaimed property.

PROCEDURE: I. GENERAL STANDARDS

A. Qualifications

- (1) The audit is to be performed by a person or persons having adequate technical training and proficiency as an auditor. Unclaimed Property Auditors should have knowledge of accounting and auditing principles and be able to apply this knowledge to an Unclaimed Property audit.
- (2) Each auditor is to have knowledge of Unclaimed Property law, both statutory and case law.
- (3) Auditors are responsible for maintaining technical competence through continuing education.

B. Independence

- (1) Auditors are to be free from personal, external, or organizational biases and must be independent in attitude and appearance.
- (2) Unclaimed Property Auditors must be independent in order to maintain the public's confidence.
- (3) If lack of independence and objectivity will impair an auditor's participation, the auditor may request that he or she not be assigned to that audit.

C. Due Professional Care

- (1) The auditor must employ professional standards in performing Unclaimed Property audits.
- (2) The auditor is to ensure that the holder is aware of the scope and objectives of the audit and should obtain a good understanding of the holder's operations.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 3

SUBJECT: GENERAL AUDIT STANDARDS **Procedure Number: 2018-20**

- (3) When selecting tests and procedures to be applied during fieldwork, the auditor should consider the audit objectives, effectiveness of internal control and cost vs. benefit of the audit work being performed.
- (4) The auditor should be alert for the mishandling of dormant funds and situations indicative of noncompliance.
- (5) The auditor is to continue fieldwork until he or she is confident that all amounts of unclaimed property have been identified.
- (6) The auditor is to follow-up at a later date on non-complying audits to ensure that corrective action has been taken by the holder.

D. Scope Impairments

- (1) When factors imposed by the holder restrict the audit or interfere with the Unclaimed Property Auditor's ability to form objective opinions, the auditor should take steps to have the limitations removed.
- (2) If the auditor is unable to remove the restrictions imposed by the holder, the auditor is to refer to Procedure 2018 - 46 "Problem Holders".
- (3) The most common impairment is the denial of access to old accounting records or the denial of interviews with key officials and employees of the organization. All impairments are to be documented.

E. Confidentiality

- (1) The Unclaimed Property Auditor is to hold in strict confidence all information concerning a holder's affairs that is acquired in the course of the audit consistent with the terms of any confidentiality Agreement with the holder.
- (2) If certain information is prohibited from general disclosure, the report shall state the nature of the information omitted and the reason for its omission.

II. FIELD STANDARDS

A. Planning

- (1) The audit agenda is to be adequately planned and discussed with staff assigned to the examination.

AUDIT SERVICES U.S., LLC

OPERATING PROCEDURES

PAGE 3 OF 3

SUBJECT: GENERAL AUDIT STANDARDS **Procedure Number: 2018-20**

- (2) Audit programs detailing step-by-step procedures are to be followed for each type of property being examined.

B. Study and Evaluation of Internal Control

- (1) The auditor is to establish a basis for reliance on internal control to determine the nature, extent, and timing of the audit tests to be applied.
- (2) The auditor should determine whether the holder has appropriate policies and procedures in place to enable it to comply with the Unclaimed Property Law.
- (3) The auditor is to provide constructive suggestions to holders concerning improvements in internal control.

C. Working Papers

- (1) Working papers are to contain the detail to support the audit findings. They are to be legible and should only include information that is relevant to the Statement of Examination Findings.
- (2) Work papers are to be numerically indexed and cross-referenced so that future auditors will be able to follow the audit trail. (See Procedure 2018-40 "Work paper Technique")

III. REPORTING STANDARDS

- A. The audit report is to state whether the holder is in compliance with the Unclaimed Property Law or in noncompliance.
- B. Scope limitation(s) should be stated in the audit report. (See Procedure 2018-46 "Problem Holders")
- C. Any material deficiencies detected during the examination are to be included in the audit report.
- D. A copy of the audit report along with supporting schedules is to be given to the States. A duplicate copy is to be maintained in the audit file.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-22**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: USE OF AUDIT PROGRAMS

PURPOSE: To describe the procedures utilizing audit programs in the performance of an unclaimed property audit.

DISCUSSION: An audit file should be prepared for each audit and is essential to conducting audits efficiently and effectively. Auditing Standards define an audit program as detailed steps and procedures to be followed in conducting an audit and preparing an audit report.

PROCEDURE: I. SELECT AUDIT PROGRAMS

- A. The Auditor-in-Charge/staff assembles audit files based on special characteristics of the holder and determines if the programs will achieve the proposed goals.
- B. Audit programs are maintained electronically and in hard copy.

II. THE AUDIT PROGRAMS PROVIDE THE FOLLOWING INFORMATION:

- A. Series of audit procedures applicable to holder.
- B. Basis for assigning work.
- C. Basis for summary of work done.

III. AUDIT PROGRAM GUIDELINES

- A. The Audit Programs are not intended to be all-inclusive; therefore, the Auditor-in-Charge must apply judgment in developing additional/alternative procedures since unique field problems may be encountered.
- B. Audit Programs should be updated based on staff experiences and changes in the unclaimed property and related statutes
- C. Two phases of the Audit Program:
 - (1) The compliance testing phase includes observation tests, detailed tests of transactions, and interviews with holder personnel.
 - (2) The substantive testing phase includes tests of the details of balances and analytical review procedures.
 - (3) The end result of completed audit programs will be an organized, understandable file and an accurate audit report.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-24**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: AUDIT FILE FORMAT

PURPOSE: To describe the procedures used in compiling the completed audit file.

DISCUSSION: All audit files need to be compiled in the following format to insure consistency and ease in reviewing.

PROCEDURE: I. GENERAL INDEX

SECTION 100

- (1) Report Guide Sheet
- (2) Managers Review Program

SECTION 200

- (1) Title page "as of" date records examined
- (2) Table of contents
- (3) Letter to holder
- (4) Statement of Examination Findings (if applicable)
- (5) Management Advisory Comments (if applicable)
- (6) Supporting schedule(s) (if applicable)

SECTION 300

- (1) Correspondence and Telephone Record
- (2) Telephone call record
- (3) Copies of all correspondence received or sent in chronological order.
- (4) Unclaimed property reports received as a result of an audit, if applicable Detail Schedule of Findings
- (5) Records Request

SECTION 400

- (1) Audit Roster
- (2) Time Allocation Report

SECTION 500

- (1) Review of Internal Control
- (2) Internal Control Questionnaire Module

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: AUDIT FILE FORMAT

Procedure Number:

2018-24

SECTION 600

- (1) Audit Program Index
- (2) Pre-Audit Steps
- (3) Audit Opening Steps
- (4) Audit Review Steps
- (5) File Review Steps

SECTION 700

- (1) Auditors Notes
- (2) Outstanding Issues
- (3) Records Request

SECTION 800

- (1) Holder information. (As applicable)
 - Holder Profile
 - Hoovers, Moody's, Capital Changes Reports, etc.
 - Annual Reports, etc.
 - Organization Chart
 - Policy and procedures of holders
 - Contracts, rules and regulation of holders.

SECTION 900

- (1) Unclaimed Property Report Analysis
- (2) U/P Report Audit Program
- (3) States which reports are filed to
- (4) Related work papers

SECTION 1000

- (1) General Ledger Review
- (2) Journal Entry Review Matrix
- (3) Chart of Accounts
- (4) Trial Balance

SECTION 1100-2000

- (1) Audit Program used
- (2) Audit Findings Schedule(s)
- (3) Supporting work papers

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-26**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: NO DATE PROPERTY

PURPOSE: To describe the procedures used to evaluate and schedule no date property.

DISCUSSION: During the course of the examination unclaimed property may be identified which cannot be adequately aged or dated due to insufficient record keeping by the holder. In these instances, an auditor must make a reasonable and supportable determination as to whether the property should be classified as demandable, reportable, or reinstatable.

PROCEDURE: I. EVALUATING PROPERTY

A. Attempt to date property based on available records by:

- (1) Examining sequence of check numbers, certificates, patient or customer numbers, any other property identification numbers.
- (2) Determining length of time present chart of accounts or selected accounts have been in use.
- (3) Establishing conversion date.
- (4) Reviewing operational characteristics of holder including stock offerings, new product offerings, the opening of new stores, plants, etc.
- (5) Analyzing holder's reporting history.

II. SCHEDULING PROPERTY

- A. Provided that the preceding evaluations were performed and given that current records are generally more accurate than historical records, any property which cannot be reasonably dated will be treated as demandable subject to the requested research of the holder. Property that can be reasonably aged will be scheduled in accordance with Procedure 2018-44 "Demandable, Reportable, and Reinstatable Property".

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-28**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: NO ADDRESS PROPERTY

PURPOSE: To describe the procedures used to evaluate and schedule no address property and distribute same to the proper State.

DISCUSSION: During the course of the examination unclaimed property may be identified which cannot be adequately assigned to a State due to insufficient record keeping by the holder. In these instances, an auditor must make a reasonable and supportable determination as to which State the property should be reported to.

PROCEDURE: I. EVALUATING PROPERTY

A. Attempt to secure name and address of the owner of property based on available records by:

- (1) Examining supplemental documents such as vendor registers and employee pay records.
- (2) Determining existence of alternate sources of names and addresses such as 1099 records.

II. SCHEDULING PROPERTY

A. Provided that the preceding evaluations were performed and given that supplemental records are generally reliable, contact the States involved and get further directions.

III. NO RECORDS AVAILABLE

A. Allocate to States according to the governing court cases (See procedure 2018-38 "Auditing for Multiple States")

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: 2018-30
Effective Date: January 1, 2018
Approval: _____

SUBJECT: UNDERLYING SHARES AND THE DETERMINATION OF ABANDONMENT

PURPOSE: To describe the procedures used to evaluate and schedule underlying shares and distribute them to the proper State.

DISCUSSION: During the course of the examination the auditor will seek evidence of shares of stock that the holder has been unable to deliver to a shareholder, and shares of stock that have been issued to a shareholder and thereafter have been abandoned by the owner.

PROCEDURE: I. AUDIT PROGRAM

A. The auditor will follow the steps outlined in the audit program, which include, but are not limited to the following:

- (1) Analyze the history of the holder (i.e.: classes of stock outstanding, stock splits, stock dividends, mergers, acquisitions, etc.)
- (2) Request that the company obtain records identifying unexchanged and/or undeliverable stock certificates, outstanding dividend checks, dormant book entry accounts returned from the post office (RPO) accounts and inactive dividend reinvestment accounts, if the company uses an outside transfer agent.
- (3) Document successive periods of uncashed dividend checks and determine if underlying shares can be claimed.
- (4) Prepare spreadsheets for identifying unexchanged and underlying shareholder accounts, including:
 - a. Owner information (name, last known address, social security number, and account number, if known)
 - b. Issue name and type

II. AUDIT FINDINGS

- A. Include unclaimed property amounts due each state based on that State's statutes. When citing the underlying share as unclaimed property, the share should be claimed based on the applicable state statute (i.e. holding periods may vary).

- B. Include all categories of property.
- C. Property will be reported under terms of contract.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-32**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: BANKRUPTCY

PURPOSE: To describe the procedures used when a holder of unclaimed property files for bankruptcy.

DISCUSSION: Federal bankruptcy law does not always preempt state escheat laws. The States may have the right to stand in the shoes of the owners who cannot be located.

PROCEDURES: I. NOTICE OF BANKRUPTCY

- A. The auditor-in-charge receives notice of a corporation in bankruptcy:
 - (1) By receipt of a proof of claim form from the bankrupt.
 - (2) By notification from another vendor (Clearinghouse) or State.
 - (3) From learning of the bankruptcy through research (newspaper).
 - (4) From telephone inquiry to bankruptcy courts.

II. CONTACT STATES

- A. Contact the States involved and get further directions when:
 - (1) It is determined that a sufficient basis for making a claim exists and a proof of claim may be submitted.
 - (2) The holder (bankrupt) never filed a report or filed only negative reports and nothing suggests any possibility of a substantial claim against the bankrupt.
- B. When the auditor-in-charge has notice of a bankruptcy, Due Care should be taken that no effort is made to pursue other collection efforts or an audit of the bankrupt company in order to avoid making the bankruptcy judge angry for interfering with the conduct of the bankrupt business by the trustee and bankruptcy court.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: 2018-33
Effective Date: January 1, 2018
Approval: _____

SUBJECT: OUT OF PROOF REPORTS

PURPOSE: To describe the procedures used to evaluate and schedule out of proof reports and distribute same to the proper State.

DISCUSSION: Out of proof reports are those in which inaccurate record keeping results in more accounts listed in the report than actual accounts exist, for which property is remitted to the State at a value less than the total of the report. It is Audit Services, U.S., LLC's intent in all examinations to reconcile the property to the report; however, it recognizes that holders holding equity issues will sometimes have inadequate records to determine whether or not an owner has been previously paid. The States may find it acceptable for the holder to submit a report that is short or "out of proof."

PROCEDURE: I. ACCEPTANCE OF OUT OF PROOF REPORTS

A. Out of proof reports will only be accepted when:

- (1) Written assurances are provided by the holder that should all owners come forward, the holder will provide the balance due.
- (2) The reports are clearly marked as out of proof and the reason the report is out of proof is certified by the holder or the Holder's agent.
- (3) Approval has been received from the States involved to accept an out of proof report.

II. VERIFICATION AND NOTIFICATION

- A. When notified of an out of proof report, the auditor will verify the amount or percentage by which the report varies.
- B. The auditor-in-charge will notify the States involved of how much the holder is "out of proof" and will await further instructions or approval from the States.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-34**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: **LOCATING AND EVALUATING HISTORICAL RECORDS**

PURPOSE: To describe the procedures used in determining the oldest records required for the examination, and in locating and evaluating said records.

DISCUSSION: Due to the long-term nature of unclaimed property dormancy periods complications are continually encountered in relation to the availability of records or the lack of certain types of records.

PROCEDURE: **I. EXAMINATION SCOPE**

- A. Normally research the last five years.
- B. If noncompliance is evident, research as far back as needed or allowed by each State's law.
- C. If holder is in compliance, it is not necessary to extend the scope of the audit.
- D. If the first report filed covers the entire reach back period for all property types permissible under the law, further research is not required.

II. LOCATING RECORDS

- A. Determine that the records exist
 - (1) Examine record retention manuals.
 - (2) Interview key employees.
 - (3) Review oldest available written procedures, memos, and files.
 - (4) Establish record keeping practices from audit trail.
- B. Verify the location of the records
 - (1) Determine who has control of the records.
 - (2) Examine records storage areas.
 - (3) Inspect the records.
- C. If records are not available, have holder sign record request letter acknowledging that the records are not available.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

PROCEDURE NUMBER:

2018-34

SUBJECT: LOCATING AND EVALUATING HISTORICAL RECORDS

III. EVALUATING RECORDS

- A. Determine the existence of required records.
- B. Age available documentation and recorded activities.
- C. Decide if available documentation is adequate to calculate and support examination findings as needed.
- D. Prepare an estimate from available records if holder's record retention is inadequate and there is evidence of noncompliance and the holder is incorporated in a State that allows estimation (See Procedure 2018-36 "Estimates").

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-36**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: ESTIMATES

PURPOSE: To review the conditions and circumstances requiring the performance of estimates and to recommend procedures to be used in computing estimates.

DISCUSSION: The availability of the holder's records and cost benefit determinations may compel the audit staff or the holder's personnel to estimate the value of demandable and reportable property. For amounts in excess of the State's aggregate value, every reasonable effort should be undertaken to ensure that the reporting of all available last known names and addresses will not be jeopardized by performing an estimate.

PROCEDURE: I. CIRCUMSTANCES REQUIRING ESTIMATES

A. RECORDS UNAVAILABLE

- (1) When the holder's record retention policy limits the scope of the examination, a review of the available records should be used to estimate areas of noncompliance for the periods in which the record keeping was inadequate (See Procedure 2000-26 "No Date Property").
- (2) Have holder sign Record Request Form acknowledging that the records are not available.
- (3) Determine the method of Estimation
- (4) Have holder sign mutually agreed upon method of estimation.

B. RECORDS AVAILABLE

- (1) Circumstances may arise where the holder's record keeping is adequate, however, due to the cumbersome nature of the holder's records or to the volume of specific unclaimed property items, it may be cost beneficial to estimate the total findings in a given area. The Auditor-in-Charge should determine whether an estimate performed by the audit staff or by the holder's personnel will generate the most accurate and cost effective assessment. The States involved must approve of this plan.
- (2) Have holder sign Record Request Form
- (3) Determine the method of Estimation

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: ESTIMATES

Procedure Number:

2018-36

II. VALIDITY OF FINDINGS

- A. When holder research is not feasible or past records are not available for 100% of the findings, a sampling may be performed to determine accounting errors. The result will be applied to the total population.
- B. Inform the holder that the result of the sample will be applied to the total population.

III. PROPORTIONATE FOR MULTIPLE STATES

- A. In the event that property is due multiple states, a reapportionment may be performed.
- B. The States must approve any apportionment of names and address when records are available.
- C. Have holder sign mutually agreed upon method of estimation

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-38**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: AUDITING FOR MULTIPLE STATES

PURPOSE: To describe the procedures for identifying property belonging to various states and assuring compliance with Supreme Court cases.

DISCUSSION: Audit Services has contracts with the District of Columbia and numerous states, which call for representation during an audit. Auditors should make the holders aware of the benefits of filing one report to Audit Services rather than reporting to numerous states.

PROCEDURE: I. IDENTIFYING PROPERTY BELONGING TO VARIOUS STATES

A. Determine States in which Holder Has Filed

- (1) Through interview with holder.
- (2) "States Filed To" work paper checklist.
- (3) Reviewing previously files reports.

B. Determine States in which Holder Has Liability

- (1) Last known addresses of demandable, reinstatable and reportable property.
- (2) Rules of Texas vs. New Jersey and Delaware vs. New York.
- (3) State of incorporation.

C. Inform Holder of Our Obligation

- (1) To collect and remit to States with contracts.
- (2) To inform states of holder's potential liability.

III. AUDIT FINDINGS

- A. Include unclaimed property amounts due each state based on that State's statutes. The holder should be informed that it is the responsibility of the holder to remit property in accordance with the dormancy periods of each state.
- B. Include all categories of property.
- C. Include aggregate amounts if not incorporated in States under contract.
- D. Property will be reported under terms of contract.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

Procedure Number:

2018-38

SUBJECT: AUDITING FOR MULTIPLE STATES

D. Underlying Shares, if Applicable

- (1) Because of potential liabilities special attention should be placed on stock activities.
- (2) When citing the underlying share as unclaimed property, the share should be claimed based on the applicable state statute (i.e. holding periods may vary).

IV. Holder Chooses Not to Remit State Findings to Audit Services.

- A. Notify States of amount due.
- B. Make available work papers and documentation if requested.
- C. Assist State in any way.
- D. Holder must provide proof such as copies of checks and reports to Audit Services that they have filed to other states.

V. Resources

- A. Quick Reference Section of Guide To Unclaimed Property And Escheat Laws by Anthony L. Andreoli.
- B. Unclaimed Property Offices in each state
- C. Individual state statutes.
- D. The ASUS Auditor Training Manual

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 6

Procedure Number: **2018-40**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: WORKPAPER TECHNIQUE

PURPOSE: The purpose of work papers is to document the examination findings and the degree of compliance identified during the course of an audit.

DISCUSSION: Work papers support the basis for comments, exceptions and recommendations cited by the auditor in the report and are the historical records maintained by the auditor of work performed and findings. The form of work paper layout is a matter of individual auditor discretion. However, the auditor is expected to maintain clarity and consistently apply standard audit procedures. The intent of work papers is to display facts to other readers, not just the composing auditor.

PROCEDURE: I. WORK PAPER LAYOUT

A. SIZE

- (1) The file will be 8 1/2" X 11"
- (2) Pages should be folded/trimmed to accommodate the file size.
- (3) Work papers should all face the same way.

B. APPEARANCE

- (1) Work papers must be neat and orderly.
- (2) Work papers should be written in dark pencil, with references in red.
- (3) Notes should be written at the bottom of the page. If there is not enough space or the paper is not clear use another piece of paper to write the note and place it behind the work paper.
- (4) Only one side of the paper is to be used.

C. ORDER

- (1) SEE PROCEDURE 2000-24 "AUDIT FILE FORMAT"

D. HEADINGS

- (1) Each work paper should be headed as follows:
 - a) Top line - holder name
 - b) Following line - main subject

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 6

SUBJECT: WORKPAPER TECHNIQUE

Procedure Number:

2018-40

- c) Third line, if necessary - specific purpose
- d) Each work paper should be initialed and dated when applicable in upper right hand corner below page number by the auditor doing the work and the person reviewing the work.

E. ATTACHMENTS

- (1) Attachments
 - a) Documents should be attached neatly to the worksheet.
 - b) The attachment should reflect the holder being audited.
 - c) Attachments should be neatly trimmed and/or folded to fit the 8 1/2" x 11" audit file size.
 - d) Attachments should contain a description/explanation of its relevance to the audit.

F. PAGE NUMBERING

- (1) When numbering work papers the auditor should keep in mind that cross-references will be used. Therefore, page numbering should be simple and understandable.
- (2) Work papers are to be numbered using the work paper Index.
- (3) Work papers are to be numbered consecutively.
- (4) Page numbers should change with each new topic. Work papers relating to each topic should be subnumbered. For example:

Outstanding Checks Program (page 1)	1100
Outstanding Checks Program (page 2)	1100.01
Lead Schedule	1101
A Bank Reconciliation	1102
An Outstanding Check List	1102.01
A Bank Reconciliation	1103

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 3 OF 6

SUBJECT: WORKPAPER TECHNIQUE

Procedure Number:

2018-40

G. TICK MARKS

- (1) A TICK MARK IS A SYMBOL (LETTER, NUMBER, CHECK, MATHEMATICAL OR GEOMETRIC DESIGN) INDICATING THAT AN:
 - Audit function (foot, agree, confirm, trace, etc.) has been performed, or
 - Explanation or clarification exists in a footnote.
- (2) Always pencil tick marks in red and explanations in black.
- (3) To provide consistency in all work papers and facilitate review, the following standard tick marks should be used:

✓	Adequate, OK (a positive confirmation of the trait for which the auditor is testing)
^	Footed
<	Cross-Footed
T	Traced to outstanding checks
A	Agrees to bank statement
GL	Agrees to the general ledger
N/A	Not applicable
- (4) Explain Symbols Used: If additional tick marks are necessary, explain tick mark at the bottom of each work paper or reference to appropriate tick mark legend.

II. AUDIT PROGRAM COMPLETION

- A. Completed audit program steps are signed-off (initialed) and dated by the auditor who performed the work. All auditors working on an audit step should initial the audit program.
- B. If audit steps are added during the field work, the additional steps should be recorded on the audit program. Likewise, if steps are not applicable to the audit, a note stating the reason should be documented on the program.
- C. Tick marks are used in the reference column of the audit program when the referenced note applies to more than one step within the audit program or if there is not enough room under the audit step and must be explained elsewhere.

III. SOURCE, PURPOSE, OPINION STATEMENT (SPO)

A. SOURCE

- (1) Source of information and title of the source is reflected in the SPO. If the work papers in the section come from more than one source, each work paper should reflect the source.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 4 OF 6

SUBJECT: WORKPAPER TECHNIQUE

Procedure Number:

2018-40

B. PURPOSE

- (1) A statement is written describing the reasons for performing the audit program. The section of law should be reflected if applicable.

C. OPINION

- (1) A statement(s) is written summarizing the results of tests with references to the corresponding work papers to provide detail. A conclusion to the audit work should be written.

IV. LEAD SCHEDULE

- A. Lead Schedules are prepared for sections that contain findings.
- B. Findings are cross-referenced to the supporting documents.

V. MISCELLANEOUS TECHNIQUES

- A. The work papers should be organized and cross-referenced to provide a clear record of work performed.
- B. Narratives should be used to document any steps taken during the audit that were not included in the audit program.
- C. Bulk materials are to be organized and filed separately with an appropriate cross-reference in the working papers. Summaries pertaining to bulk material should be properly filed in the related working papers.
- D. Be sure to resolve all questions and exceptions indicated in your working papers. Occasionally, you may not be able to immediately determine the disposition of some issues. These issues should be listed on work paper 701 – Outstanding Issues.
- E. Work papers that are attached to a single work paper and folded are to be numbered as such: 1/2, 2/2.
- F. If a page contains sections unrelated to the audit they are to be neatly crossed-out in red.
- G. To reference numbers to each other on the same work paper; small circles with corresponding letters and arrows are to be used. Example:

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 5 OF 6

SUBJECT: WORKPAPER TECHNIQUE

Procedure Number:

2018-40

VI. WORKPAPER REVIEW NOTES

A. PREPARATION

- (1) Review notes are prepared by the Director of Audits. Review notes are recorded on the work paper review note form with the name of the review note preparer and the auditor responsible for follow-up at the top of each page. If no review notes result from the review process, a review note sheet is not necessary.

B. CLEARANCE

- (1) The auditor is responsible for clearance of their own review notes and any others which are assigned. The auditor should write their responses to the review note in the comment column of the review note sheet. The auditor should also provide the corresponding review note number to his response to facilitate assurance that all review notes were addressed. If another auditor clears the review note, the auditor is to initial the response to provide accountability. Occasionally, the auditor clearing the review note will make an addition or correction to a work paper other than the page indicated in the review note. For these instances, the auditor clearing the note indicates where work was performed.

C. FOLLOW-UP

- (1) Review note follow-up should be completed as soon as possible to avoid interference in other projects. When the note is cleared it is crossed out with a red "I". If the follow-up has been delegated, the individual completing the follow-up includes his initials with the "I" for accountability. When all review notes have been cleared they are retained by the audit manager.

VII. WORKING PAPER DEFICIENCIES

- A. For the most part, working paper deficiencies result when an auditor neglects one or more of these responsibilities:

- (1) Organizing the working papers properly
- (2) Rechecking all important calculations
- (3) Bringing exceptions to the attention of the auditor-in-charge and obtaining his acknowledgment of them.
- (4) Clearing exceptions noted in the working papers or carrying them forward to a pending matters list

- (5) Indexing all working papers properly. This procedure includes a clear logical system of numbering and the reflection in the cross-reference of all numbering changes

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 6 OF 6

SUBJECT: WORKPAPER TECHNIQUE

Procedure Number:

2018-40

- (6) Using clear and logical working paper headings
- (7) Signing and properly dating work papers
- (8) Disclosing conclusions on the accounts being analyzed
- (9) Footing or test footing auditor prepared schedules
- (10) Explaining audit tick marks
- (11) Indicating sources of information where appropriate
- (12) Transcribing only useful information onto the working papers
- (13) Understanding the overall objective of an audit procedure, thereby ensuring against the mechanical performance of unimportant tasks
- (14) Recording accurately and legibly information to be used in confirmation requests (e.g., serial numbers, names, dates, property descriptions, amounts). All this information should be entered on working papers with extreme accuracy and should be suitable in all respects for transfer to confirmations.

Each of these items should be considered when performing a self-review of work papers.

AUDIT SERVICES, U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-42**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: DOCUMENTATION REQUIREMENTS

PURPOSE: To describe the procedures for adequately documenting the audit steps performed.

DISCUSSION: Auditing standards require that sufficient, competent evidence be obtained by the auditor. The auditor must seek evidence that in their professional judgment is relevant and reliable. Examination of this evidence must be documented in the work papers (See Procedure 2018-40 "Work paper Technique"). A file of the audit findings is maintained as a permanent record.

PROCEDURE: I. DOCUMENTING AUDIT PROCEDURES AND FINDINGS

- A. The following definitions, principles, and concepts are to be considered when documenting audit procedures and findings:
- (1) Selectivity - The auditor should select information sufficient to draw an accurate conclusion.
 - (2) Reliability - The documentation should be reliable. It is important to remember that information such as oral statements, written statements, procedures, etc. are to be verified as to what is actually happening, not what should be happening.
 - (3) Relevance - The documentation must directly support an audit step or finding.
 - (4) Sufficiency - The quantity of documentation is usually a judgment call made by the auditor based on their experience. It is logical to say more documentation is required to support findings in areas of possible dispute.

AUDIT SERVICES, U.S., L.L.C.

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-44**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: DEMANDABLE, REPORTABLE, AND REINSTATABLE PROPERTY

PURPOSE: To describe the property classifications used in the “Statement of Examination Findings” which serve to inform the holder of the status of the various items of unclaimed property.

DISCUSSION: In order to assist the holder in complying with the audit findings, unclaimed property identified during the audit is divided into the following three classifications: Demandable, Reportable, and Reinstatable. By placing the property into these classifications, the holder is better able to account for the property and report it when due.

PROCEDURE: I. DEMANDABLE PROPERTY

- A. Include in this category property that should have been paid or delivered to the States in prior years. The holder may deduct from this amount any property that is returned to the rightful owner or deemed accounting errors.

II. REPORTABLE PROPERTY

- A. Include in this category property that is still on the books of the holder (credit balances, outstanding checks, etc.) which should be reported to the proper State in the future. The holder may deduct from the audit findings any amounts that are returned to the rightful owner or deemed accounting errors.

III. REINSTATABLE PROPERTY

- A. Include in this category unclaimed property due to the proper State in future years that the holder has taken into income. This amount, less any items returned to the rightful owner or deemed accounting errors, will be reportable in the future based on the applicable statutory holding period.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 3

Procedure Number: **2018-46**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: PROBLEM HOLDERS

PURPOSE: To develop guidelines for auditing holders who view an unclaimed property audit as an inconvenience and are not cooperative.

DISCUSSION: An occasion may arise where the holder does not agree with:

- the need to file a report
- the scope of the audit
- the records requested
- the property identified.

When this occurs the auditor needs to maintain professional decorum. The auditor should be aware of any possible legal implications that may arise as a result of the audit and document all discussions with the holder that take place before, during, and after the audit. It may be necessary to more fully document the audit work performed in order to fully support audit conclusions for discussion with problem holders.

PROCEDURE: I. THE AUDIT TEAM SHOULD BE KNOWLEDGEABLE OF:

A. Holder's Attitude Before the Audit

- (1) If holder attempts to delay audit
 - a. Be polite
 - b. Offer a choice of two dates
 - c. Select a date and set an arrival time
- (2) If holder objects to records requested
 - a. Submit a records request
 - b. Adhere to normal audit routine
 - c. Expand as necessary to obtain information
- (3) If holder protests types of property to be reviewed
 - a. Use the State unclaimed property manuals to illustrate types of property.
 - b. Refer to applicable paragraphs in the statute

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 3

SUBJECT: PROBLEM HOLDERS

Procedure Number:

2018-46

B. Holder Conduct During the Audit

- (1) Working conditions intolerable
 - a. Request more appropriate conditions
 - b. Consider general conditions available
- (2) Holder delays in obtaining requested information
 - a. Access to record areas speeds audit process
 - b. Remain on site to see if records arrive
 - c. Leave record request
 - d. Set a time to return to review records
- (3) Holder denies access to employees who prepare records and/or record storage areas
 - a. Remind holder that the audit will proceed faster
 - b. Refer to statutes on the examination of records

C. Holder Conduct After the Audit

- (1) Protest audit (See Procedure 2018-58 - "Audit Protest")
- (2) Disagree with findings
 - a. Review each area with holder
 - b. Negotiate compromise (with administration's approval)
- (3) Review with holder possible penalty for failure to file

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 3 OF 3

SUBJECT: PROBLEM HOLDERS

Procedure Number:

2018-46

II. COMMUNICATION WITH HOLDER DURING AUDIT

- A. Adhere to the Statutes
- B. Be consistent-refer to conclusions reached on prior audits
- C. Keep holder informed during the audit
- D. When issues are uncertain, research and follow up with the holder later
- E. Record in auditor's notes all discussions taking place during the audit
- F. Give holder schedules of property identified (if possible, Statement of Examination Findings) at conclusion of field work
- G. Request records needed to complete audit

III. AUDITOR INVOLVEMENT

- A. Keep Director of Audits informed of any problems encountered during the audit
- B. Make Audit Contact aware of inappropriate conduct of holder employees

IV. HOSTILE HOLDER

- A. Under no circumstances does the audit staff tolerate abusive language from the holder.
- B. Explain that if abuse does not stop, the audit staff will vacate immediately and report back to management.
- C. Document the nature of abuse and the employee administering the abuse.

VI. KEEP STATES INFORMED

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-48**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: CONCURRENT AUDITS - CONFLICTS AND RESOLUTION

PURPOSE: To develop guidelines for eliminating and resolving possible disputes with other vendors when auditing holders who are also being audited by another vendor.

DISCUSSION: An occasion may arise where the holder or agent of the holder is being audit concurrently as Audit Services is conducting an audit.

PROCEDURE: I. PROCEDURE TO FOLLOW WHEN A CONFLICT OCCURS WITH ANOTHER VENDOR

A. COMMUNICATION

- (1) Inquire of the holder whether another vendor is auditing a division, branch, subsidiary, or a third party administrator or paying agent.
- (2) Authorizations to audit and audit notification letters inform the States of an impending audit by ASUS.
- (3) A quarterly Status Report informs the States of ASUS's audit candidate list and intentions to audit holders.
- (4) When ASUS is aware of a conflict, management will immediately contact the other vendor and try to resolve the matter without getting the States involved.

II. VOLUNTARY VS. INVOLUNTARY AUDITS

- (1) An involuntary audit takes precedence over a voluntary compliance when the contact dates are the same.
- (2) The vendor with the earliest State approval is considered by ASUS as the approved contractor.
- (3) When two contact persons from the same holder are contacted by different vendors at the same time, the States will decide who they want to work with. (Or the contact person with the highest authority will take precedence.)
- (4) When different subsidiaries or divisions are contacted by different vendors at the same time, the States will decide who they want to work with. (Or the contact person with the highest authority will take precedence.)

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

Procedure Number:

2018-48

SUBJECT: CONCURRENT AUDITS - CONFLICTS & RESOLUTION

- (5) A CPA firm bringing a holder into voluntary compliance is not considering a conflict. Ask for directions of the States.

IV. GENERAL LEDGER VS. EQUITY

- A. When auditing a holder and a request for records from a third party agent has been made and same agent goes through another vendor, ASUS takes the position that any monies received by the states are as a result of ASUS audit efforts.
- B. When auditing a third party records and the third party routinely reports through another vendor. Any monies that would not have been turned over routinely by the agent are considered as a result of ASUS audit efforts.

V. STATES DIRECTIONS

- A. State instructions take precedence over any subsequent procedure

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-50**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: AUDIT REPORT

PURPOSE: To describe the procedures used in preparing a standardized audit report of unclaimed property.

DISCUSSION: After audit fieldwork is completed, a closing conference is held with holder personnel. At this time, a rough draft of the Statement of Examination Findings and/or supporting schedules are furnished to the holder and explained in detail. A completed audit report is prepared upon returning to the office and mailed to holder and to each State represented.

PROCEDURE: I. COMPLETE AUDIT REPORT

A. TITLE PAGE

- (1) Holder's name, subsidiaries, FIN, city and state
- (2) Audit Cut-Off Date

B. CONTENTS PAGE

- (1) Letter to Administrator
- (2) Statement of Examination Findings
- (3) Management Advisory Comments
- (4) Schedules of Examination Findings

C. LETTER TO HOLDER

- (1) Non-Compliance Letter - If holder is not in compliance with the Unclaimed Property Law.
- (2) Compliance Letter - If holder is in compliance with the Property Law.

D. STATEMENT OF EXAMINATION FINDINGS

- (1) Property should be listed by type and due date and is categorized as demandable, reportable, and/or reinstatable.
- (2) Definitions for amounts demandable, reportable, and reinstatable are at the bottom of the page.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: AUDIT REPORT

Procedure Number:

2018-50

E. MANAGEMENT ADVISORY COMMENTS

- (1) Includes any reporting or internal control weaknesses noted during the audit, and references appropriate paragraph of statute.
- (2) Condition is stated and followed by a recommendation.
- (3) Holder response to recommendation, if necessary.

F. SCHEDULES TO SUPPORT STATEMENT OF EXAMINATIONS FINDINGS, AS NEEDED.

AUDIT SERVICES U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-52**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: AMENDED FINDINGS

PURPOSE: To describe the procedures employed in the receipt of amended figures to audit findings.

DISCUSSION: After audit field work is completed the holder furnishes the audit staff additional documentation which may amend the audit report.

PROCEDURE: I. AMMENDING FIGURES TO AUDIT FINDINGS

A. MINIMUM ADJUSTMENTS - VOLUMINOUS SCHEDULE:

- (1) Strike through changes with diagonal line.
- (2) Strike through page totals with diagonal line and record new total.
- (3) Alter or strike through all schedules and audit report.
- (4) Use sufficient tick marks and notations.

B. AFTER FIELD WORK AND BEFORE AUDIT REPORT IS ISSUED:

- (1) Verify and reconcile amended documentation to the original work papers.
- (2) Place amended work papers and documentation in front of original work papers using the same work paper numbers with a prefix "A" denoting amended.
- (3) Change lead schedules by striking through original findings and replace with amended figures. (NOTE sections accordingly)
- (4) If on computer worksheet, amend figures.
- (5) Prepare audit report and audit remittance control using amended figures.

C. AFTER AUDIT REPORT IS ISSUED:

- (1) Verify and reconcile amended documentation to the original work papers.
- (2) Place amended work papers and documentation in front of original work papers using the same work paper numbers with a prefix "A".

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: AMENDED FINDINGS

Procedure Number:

2018-52

- (3) Place amended lead schedule in front of original schedule using the same work paper number with an "A" prefix. Strike through original schedule with a diagonal line and Note accordingly.
- (4) Place amended audit report section in front of original schedule using the same work paper number with an "A" prefix. Strike through original schedule with a diagonal line and Note accordingly.
- (5) Place amended Audit remittance by State in front of original schedule using the same work paper number with an "A" prefix. Strike through original schedule with a diagonal line and Note accordingly.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-54**

Effective Date: **January 1, 2018**

Approval: _____

SUBJECT: AUDIT REVIEW

PURPOSE: To describe the procedures for reviewing the audit file upon completion of the audit.

DISCUSSION: The work performed by each auditor should be reviewed to determine whether it was adequately performed and to evaluate whether the results are consistent with the conclusions presented in the Statement of Examination Findings.

PROCEDURE: I. PURPOSE OF AUDIT REVIEW

- A. Audit complies with Unclaimed Property Audit Procedures
- B. Quality Control
 - (1) Ensure standards of the department have been met
 - (2) Work papers are of professional quality and fully support the work performed and conclusions reached
- C. Consistency in application of General Statutes
- D. Training tool for auditors
 - (1) The use of review notes to instruct staff provides an opportunity to improve their performance and inform them of things they do well.
 - (2) Positive notes will provide motivation and instruction
- E. Reduce audit time
Minimize audit time thereby reducing audit cost
- F. Future planning
 - (1) Recommendations to change audit program
 - (2) Eliminate or change certain work papers
 - (3) Reduce sample size

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: AUDIT REVIEW

Procedure Number:

2018-54

II. STAGES OF AUDIT REVIEW

A. Preparer/Auditor-in-Charge

- (1) Auditor reviews own work papers
- (2) Ensure that the Statement of Examination Findings is well supported
- (3) Audit covers all predetermined areas sufficiently

B. Director of Audits

- (1) Planned direction of audit was maintained
- (2) Policies of the department were adhered to
- (3) Overall quality of the audit was sufficient

C. Attorney as Needed

- (1) Protest
- (2) Court

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-55**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: FOLLOW-UP AUDIT FINDINGS

PURPOSE: To describe procedures used to ensure that the holder responds timely to a report of findings at the conclusion of an audit.

DISCUSSION: The date for a holder to respond to or comply with an audit is stated in the audit report. The audit contact is expected to make arrangements for remittance of the proper amount within the specified timeframe.

PROCEDURE: I. AUDIT REPORT

- A. The agreed upon date of compliance is to be included in the audit report that is mailed to the holder. (Maximum period granted for compliance - 120 days). If the holder requests more time, extensions may be granted with States' approval, but interest may be accruing after 120 days.
- B. The Auditor-In-Charge records all audit findings and the agreed date of compliance in the auditor's notes. These amounts reconcile to audit report.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-56**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: REMITTANCE OF PROPERTY FROM HOLDER

PURPOSE: To describe procedures used to ensure that the holder remits the proper amount in a manner amenable to Audit Services in the interest of audit efficiency and accountability.

DISCUSSION: It is the responsibility of the Auditor-in-Charge to oversee proper remittance of funds by the holder. In most instances it is essential that funds be remitted through Audit Services to accommodate the states that require us to retain our fee from the property delivered.

PROCEDURE: PROVIDE INSTRUCTIONS TO HOLDER

- A. The Holder is encouraged to follow either of two methods for remittance of cash and two methods for remittance of securities. Cash can be remitted as a check, made payable to: "Audit Services, U.S., LLC, in trust for Unclaimed Funds" which is deposited in an interest bearing account in trust for the state immediately upon receipt. Or cash can be remitted by Wire Transfer into that same account. If the Holder prefers to wire funds they are provided with wire instructions for doing so. Securities must first be registered in the name of the state or its nominee. Then securities can be transferred by DTC or the physical securities can be delivered to our custodian bank until remittance by Audit Services to the state.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-57**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: SUBMISSION OF DATA BY HOLDER

PURPOSE: To coordinate transfer of data related to audit findings from the holders books and records to Audit Services' Data Processing Department in order to be able create report files of the proscribed type for each state the reflect accurately the findings of the audit.

DISCUSSION: It is the responsibility of the Auditor-in-Charge to coordinate with the sometimes numerous sources of data at the holder to facilitate delivery of data to Audit Services that is intelligible to Audit Services' Data Processing Department and properly represents the audit findings in the interest of audit efficiency and accountability.

PROCEDURE: I. EVALUATE AVAILABILITY OF DATA FROM HOLDER

- A. The Auditor-In-Charge is responsible for determining what data is available in electronic formats and which is only accessible from paper records.
- B. The Auditor-In-Charge will coordinate with the holder's data processors to provide all available electronic data representing the unclaimed funds to be processed. Audit Services Data Processing Supervisor is available for any technical consultation that will facilitate this coordination.
- C. The Auditor-In-Charge will coordinate with the holder's accounting personnel to generate electronic forms of data previously available only from paper records. The Auditor-in-Charge will consult with Audit Services Data Processing Supervisor to ensure that data formats created will contain the necessary information for processing and be in a form that will be practical and efficient for Audit Services use.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: SUBMISSION OF DATA BY HOLDER Procedure Number:

2018-57

II. TRANSFER OF DATA FROM HOLDER

- A. The Auditor-in-Charge will provide instructions to the holder as to how to submit the relevant data to Audit Services. In most cases the relevant data will already be incorporated into the files and work papers that have been accumulated during the course of the audit. Occasionally, as a result of research and due diligence, the difference between potential findings and actual findings is considerable and the creation of additional data files that represent the final results of the audit is practical.
- B. When final data files can be assembled during on site field work these files can be transferred securely using standard media such as diskettes or CD's. If final data files need to be assembled after all field work has been completed, the Auditor-in-Charge will instruct the holder to transfer files to himself/herself using secure FTP methods to be reviewed and reconciled to the audit work papers.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-58**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: FINAL RECONCILIATION OF AUDIT FINDINGS

PURPOSE: To ascertain that the property received, to be delivered to the state, and the related data reflect accurately the findings of the audit.

DISCUSSION: It is the responsibility of the Auditor-in-Charge to coordinate with Audit Services data processing and accounting functions to determine that the data and property received reconcile to the audit findings and to each other prior to creation of data reports for the state.

PROCEDURE: I. FINAL RECONCILIATION

- A. When the report with remittance is received, the Administrative Assistant delivers a copy of the report and the related audit file to the Auditor-in-Charge to review.
- B. The Auditor-in-Charge will compare the report to the "Statement of Examination Findings".
 - (1) Tick mark the work papers with an EYY ("YY" being the fiscal year of receipt which is the first two digits of receipt number) for the items remitted. (Example E98 is for the 98/99 fiscal year).
 - (2) For items not remitted due to the owner being located, put OLYY ("YY" being the fiscal year of notification that owner was located) beside the items on the work papers. (Example OL98)
 - (3) For items not remitted due to an accounting error, put AEYY ("YY" being the fiscal year of notification that an error was detected) beside the items on the work papers. (Example AE98)
 - (4) For items not remitted with an explanation as to their exclusion, contact the holder to determine the status of the items. Document the conversation in the audit file.

AUDIT SERVICES U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: FINAL RECONCILIATION

Procedure Number:

2018-58

- (5) If report disagrees with findings, place a copy of the report in the work papers.

NOTE: All tick marks made during review should be done in blue pencil.

- C. If satisfied with the report, the Auditor-in-Charge will update the Audit Remittance Control Sheet. The Auditor-in-Charge will then complete an Activity Report Control Sheet. The audit file and the Activity Report Control Sheet are given to the office manager to be included on the Monthly Work in Progress Report.
- D. If not satisfied with the report, the Auditor-in-Charge will consult with the Director of Audits and the holder to reconcile any differences. The audit file will remain open until all areas are resolved.
- E. If, after demandable amounts are received, reportable and/or reinstatable amounts remain due in future years, the audit file is placed in the open files. (See Procedure 2018-66 "Filing")
- F. When all findings have been reconciled, the Auditor-in-Charge will close the audit file. (See Procedure 2018-66 "Filing")

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-59**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: **PROCESS UNCLAIMED PROPERTY DATA**

PURPOSE: To create reports to be delivered to the state in the proscribed form and format which reflect the audit findings accurately.

DISCUSSION: Audit Services is charged with the responsibility of providing audit reports in various forms and formats as required by the numerous states to which we provide Unclaimed Property recovery services. Audit Services' data processing function is responsible for maintaining that expertise and keeping current on changes in state requirements.

PROCEDURE: **I. PROCESS UNCLAIMED PROPERTY DATA**

- A. When the Auditor-in-Charge has confirmed that the data on file agrees with the audit findings and that the property to be delivered has been remitted to Audit Services, he/she informs the data processing department that production of report files can be scheduled.
- B. The Data Processing Supervisor prioritizes and schedules production of the report files as appropriate, taking into consideration all production currently scheduled.
- C. When production commences, the Data Processing Department, using Audit Services proprietary *Audit Services System*, imports all the relevant data to be processed. The data is analyzed to ascertain that all required information is included in the data and that the data is properly formatted for processing.

AUDIT SERVICES U.S., LLC

OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: PROCESS UNCLAIMED PROPERTY DATA Procedure Number: 2018-59

- D. Once the data is prepared for processing, the NAPS system generates each state's report file in each state's proscribed format (primarily NAUPA standard format on diskette but also any state proprietary formats and media) along with all supplemental schedules that are required by individual states. These supplemental schedules may include a detailed paper report of the contents of the electronic data file, a paper replica of a state's report form(s), and various state mandated certification pages.
- E. The diskettes and all supplemental reports and forms are forwarded to the accounting function for final processing. Each diskette is submitted to a quality control review by the accounting section. The diskettes are checked for readability of the file, accuracy of the data and reconciliation to the property to be delivered. All supplemental schedules receive a visual inspection for accuracy and completeness of the information presented.
- F. When all elements have passed quality control, the materials are approved by the Accounting Supervisor for assembly and delivery.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: 2018-60

Effective Date: January 1, 2018

Approval: _____

SUBJECT: REPORT AND REMIT UNCLAIMED PROPERTY

PURPOSE: To deliver in a timely and efficient manner the unclaimed property recovered as a result of the audit and the related data.

DISCUSSION: Audit Services' accounting function is responsible for assembling, reviewing, and preparing for delivery a packet for each state that receives property from each audit.

PROCEDURE: I. REPORT AND REMIT UNCLAIMED PROPERTY

- A. Documentation and other required materials to be included in each state's packet are assembled by the accounting function. Documentation contained in all packets includes a check payable to the state, or the state's designee, for the cash property being delivered and certificates for any securities being physically delivered, an invoice for our services, and a cover letter addressed to the appropriate administrator describing the contents of the packet and identifying the holder audited. Additional documentation or other materials include the report data (on electronic media, paper, or both), description or documentation of any property being delivered directly to the state, and any specific forms required by specific states to accompany or certify the report being submitted.
- B. The accuracy and completeness of all documentation to be submitted to each state is confirmed by an accounting manager or supervisor.
- C. The reports and remittances are forwarded to the appropriate state personnel as designated by each state in their instructions to Audit Services, U.S., LLC as an authorized vendor of unclaimed property identification, recovery, processing and delivery services.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-61**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: FOLLOW-UP WHEN NO REPORT RECEIVED

PURPOSE: To recognize and respond appropriately when a holder has not remitted the agreed audit findings by the established deadline.

DISCUSSION: A holder may fail to remit reportable property for a variety of reasons. It is the responsibility of the Auditor-in-Charge, with the support of Audit Services' administrative staff, to manage the progress of each of his/her audits at each stage of the audit. If a holder has failed to timely remit property, the Auditor-in-charge is the appropriate person to ascertain the reason and rectify the failure.

PROCEDURE: I. NO REPORT RECEIVED

- A. Beginning each month, the office manager obtains remaining outstanding files that were due on or before the current report cycle.
- B. Office Manager reviews the Work in Progress Report to ensure that a report has not been received.
 - (1) If a report has been received, return to Final Reconciliation above.
 - (2) If no report has been received, the audit file is given to the Auditor-in-Charge to handle.
- C. Auditor-in-Charge sends a follow-up letter giving the holder 30 days to respond to the audit findings that were due.
- D. Auditor-in-Charge gives audit file back to the Office Manager to file.
- E. If the holder does not respond within 30 days, the Auditor-in-Charge gives audit file to the Director of Audits to send a second follow-up letter via certified-return receipt requested. A copy of the letter is placed in work papers.
- F. Director of Audits gives audit file back to the Office Manager to file.

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: FOLLOW-UP WHEN NO REPORT RECEIVED **Procedure Number: 2018-61**

- G. Director of Audits receives the green return receipt requested card and attaches the green card to the letter in correspondence section of the audit file.
- H. If a report is received, return to Procedure II above
- I. In no report is received within 30 days from the second follow-up letter, the Auditor-in-Charge will proceed with Procedure 2018-58 "Audit Protest."

AUDIT SERVICES U.S., LLC OPERATING PROCEDURES

PAGE 1 OF 2

Procedure Number: **2018-64**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: **AUDIT PROTEST**

PURPOSE: To describe the procedures used in handling a protest from the holder responding to audit findings.

DISCUSSION: Occasionally, the holder will not provide records requested, including research or a legal issue will arise that will hinder the field work until resolved. The following sequential plan of action should be employed in order to reach an understanding with the auditee.

PROCEDURE: **I. INSUFFICIENT INFORMATION/RECORDS TO ISSUE REPORT:**

- A. Discuss with holder at closing the approximate time needed to obtain information such as company research, or records needed to complete the audit (Maximum period granted is 120 days).
- B. Advise holder that interest may begin to accrue if information/records are not received by the agreed upon date.
- C. If information/records are not submitted by due date, a certified return receipt requested letter is sent advising holder that interest will begin accruing in ten business days unless information/records are submitted.
- D. If no response within ten business days, proceed to inform the States involved for directions.

II. SUFFICIENT INFORMATION/RECORDS AVAILABLE

- A. Records are available to issue report and all the evidential matter relevant to the issue involved including holder's position, legal opinions, minutes, contracts and correspondence.
- B. Legal issues raised at the closing conference outside the realm of General Statutes will usually indicate to the auditor that the holder is not willing to comply. Since the auditor does not possess legal skills, no judgments concerning information brought to his attention should be made at this time.
- C. Refer all disputed facts to Director of Audits and/or Attorney for an opinion.

AUDIT SERVICES, U.S., LLC OPERATING PROCEDURES

PAGE 2 OF 2

SUBJECT: AUDIT PROTEST

Procedure Number:

2018-64

- D. Discuss all disputed facts with State administrators, reach a conclusion, release audit report and, as appropriate demand payment.
- E. If holder is unwilling to comply at this point, attempt to schedule a meeting with the following:
 - (1) Between holder and Director of Audits
 - (2) Between holder and Key State Administrator
 - (3) Between holder and legal council
- F. If holder is still unwilling to comply, the states have to consider a course of action.
- G. If any State brings an action to compel compliance under their General Statutes.
 - (1) Director of Audits or AIC should send any work papers that may be of assistance to the State's efforts.
 - (2) Give audit information to State's legal counsel to file court order against company and/or personnel requiring their presentment of records and/or payment.

AUDIT SERVICES U.S., LLC

OPERATING PROCEDURES

PAGE 1 OF 1

Procedure Number: **2018-66**
Effective Date: **January 1, 2018**
Approval: _____

SUBJECT: FILING AND MAINTENANCE OF AUDIT FILES

PURPOSE: To describe the procedures used to maintain audit files and to provide accurate accounting records for reference purposes.

DISCUSSION: The proper maintenance of audit files is essential since they provide the means for tracing subsequent reports from holders in order to ensure compliance.

PROCEDURE: I. SUBSEQUENT TO THE AUDIT

- A. Auditor-in-Charge completes the audit file and prepares an audit report to be sent to holder
- B. Auditor-in-Charge gives Office Manager the necessary information for the quarterly WIP report and the completed audit file.
- C. Office Manager records information on the work in progress report.
- D. Office Manager places the audit file in the year of remittance due or the closed file alphabetically.

II. MAINTENANCE OF FILES

- A. The Audit Section reviews the incoming Unclaimed Property receipts for reports received as a result of an audit. Funds are deposited daily.
- B. Office Manager copies reports related to an audit and gives same and audit file to the Auditor-in-Charge for review.
- C. Auditor-in-Charge reviews the reports, makes necessary notes in the audit file and returns audit file and a completed Status(?) Report Sheet to the Office Manager to record findings on the Work in Progress report.
- D. Office Manager places audit file to the year that a remittance is due file if there are findings due in future years. If there are no more findings due, the audit file is placed in the closed file alphabetically.

III. CLOSING THE AUDIT

- A. Auditor-in-Charge determines if a file should be closed and indicates such on the Status Sheet and gives file to the Office Manager.
- B. Office Manager places the closed file in the proper file alphabetically.

ASUS EXHIBIT D

Information
Security
Policy

Audit Services U.S., LLC

Information Security Policy

Audit Services U.S., LLC (the "Company")

INFORMATION SECURITY POLICY

Key points of this Policy:

- The Company must collect, retain, access, store and dispose of the Company information in a manner that protects its security and confidentiality, based on the sensitivity of such information.
- Access to the Company information and systems must be limited to those who require such access to perform their job duties or contractual obligations.
- The Company must conduct due diligence on third parties who will be provided access to (i) the Company systems that contain Confidential Information or (ii) Sensitive Personal Information. A third party who will be provided access to Confidential Information must enter into a written agreement that requires it to protect such information.
- The Company must follow specified procedures to encrypt certain types of Confidential Information and all Sensitive Personal Information that is transmitted electronically outside of the Company (other than by fax or telephone).
- The Company must follow specified procedures to report any suspected or actual incident of unauthorized access to the Company information or systems.
- All pre-existing information security policy or requirements remain effective until expressly superseded by the new procedures, standards and guidelines that are issued pursuant to this policy. This policy will prevail with respect to any inconsistency with such pre-existing policies.

Purpose:

- To help the Company protect the security and confidentiality of the Company information and information systems, ensure continuity of business, comply with applicable legal requirements and minimize the risk of security incidents that could cause harm to the Company.

Table of Contents

1.0 PURPOSE AND SCOPE	4
2.0 APPLICABILITY	4
3.0 RELATED POLICIES, PROCEDURES AND OTHER DOCUMENTS	4
4.0 BACKGROUND	4
5.0 RESPONSIBILITIES	4
5.0 OWNER OF THE SECURITY POLICY	4
5.2 COMPANY INFORMATION SYSTEM OWNER.....	4
5.3 USERS.....	5
6.0 DEFINITIONS.....	5
7.0 OWNERSHIP AND EXPECTATION OF PRIVACY.....	6
8.0 INFORMATION MANAGEMENT.....	6
8.1 INFORMATION COLLECTION	6
8.2 INFORMATION RETENTION.....	6
8.3 INFORMATION ACCESS.....	6
8.4 INFORMATION STORAGE	7
8.5 INFORMATION DISPOSAL	7
9.0 RISK ASSESSMENT	7
9.1 ASSESSING SECURITY RISK.....	7
10.0 THIRD-PARTY ACCESS.....	7
10.1 GENERAL STATEMENT	7
10.2 WRITTEN AGREEMENT	7
10.3 WRITTEN AGREEMENT CONTENTS	7
10.4 REVIEW	8
11.0 HUMAN RESOURCES SECURITY.....	8
11.1 PRIOR TO EMPLOYMENT	8
11.2 DURING EMPLOYMENT.....	8
11.3 TERMINATION OR CHANGE OF EMPLOYMENT.....	8
12.0 PHYSICAL AND ENVIRONMENTAL SECURITY.....	8
13.0 ELECTRONIC SECURITY.....	8
14.0 INFORMATION SECURITY INCIDENT MANAGEMENT	9
14.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES.....	9
14.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS.....	9
16.0 COMPLIANCE	9
17.0 LOCATION OF OFFICIAL VERSIONS	9
18.0 EXCEPTIONS/APPROVALS.....	9
19.0 CONTACT	9
DOCUMENT CONTROL/REVISION HISTORY	10
APPROVALS /SIGNOFF	10

1.0 PURPOSE AND SCOPE

The purpose of this policy is to outline the key high-level information security policies for the Company. Company Information and the Company Information Systems, as defined herein, are assets that the organization has a duty and responsibility to protect. The confidentiality, integrity and availability of the Company Information and the Company Information Systems are essential to the Company operating in an efficient manner.

This policy is designed to protect the security and confidentiality of the Company Information and the Company Information Systems in order to, among other things, comply with applicable law, ensure the continuity of business, and minimize the risk of harm to the Company by preventing security incidents and reducing their potential impact.

This Security Policy will become effective as of the date of issuance.

2.0 APPLICABILITY

This policy applies to all Supervised Persons, contractors, consultants, temporaries, per diems, and other workers at the Company. These policies apply to all equipment, software, data, and systems that are owned or leased by the Company.

If the Company is subject to a law that establishes a higher or more detailed standard than provided in this Security Policy, the Company must comply with such law.

3.0 RELATED POLICIES, PROCEDURES AND OTHER DOCUMENTS

This policy represents the foundation of the Company framework for information security and is designed to comply with the legal requirements to which the Company is subject. This Security Policy provides a foundation for the various Company information security procedures, standards, and guidelines.

Supporting information security procedures, standards, and guidelines will be created as needed to support the Company's information security efforts.

4.0 BACKGROUND

This Security Policy is designed to protect the confidentiality, integrity, and availability of the Company Information and the Company Information Systems:

Confidentiality: ensuring that the Company Information and the Company Information Systems are secure and accessible only to those authorized to have access;

Integrity: safeguarding the accuracy and completeness of the Company Information, the Company Information Systems, and processing methods;

Availability: ensuring that authorized users have access to the Company Information and the Company Information Systems when required.

5.0 RESPONSIBILITIES

5.0 OWNER OF THE SECURITY POLICY

The Director of Operations is the owner of the Security Policy (this document), and holds the primary responsibility to administer the information security at the Company.

5.2 COMPANY INFORMATION SYSTEM OWNER

As the Company Information System owner, and in consultation with any designated IT consultants, the Director of Operations, or his designee, is responsible for purchasing requirements, development

and maintenance of information and related information systems, and as such, must define which users or user groups are allowed access to the information.

5.3 USERS

Users ("User" is defined as all Supervised Persons of the Company and any other person to whom access to the Company systems is granted.) are responsible for reading and complying with the Company IT regulations, specifically

Each User is responsible for:

- Being aware of the contents of this Security Policy and the related procedures, standards and guidelines that are applicable to him or her ("Applicable Procedures");
- Ensuring that his or her actions comply with the requirements of this Security Policy and the applicable procedures, standards and guidelines;
- Completing any required training regarding this Security Policy and its Applicable Procedures, as administered by the Director of Operations or his designee;
- Asking questions of the Director of Operations when uncertain of how to comply with the requirements of this Security Policy and the applicable procedures, standards and guidelines; and
- Reporting any violations to the Director of Operations or his designee.
- Certifying to his or her understanding of this Security Policy and the applicable procedures, standards and guidelines through the means used by the Company for such certification.

6.0 DEFINITIONS

6.1 **"The Company Information"** is any information that is collected, used or maintained by the Company regardless of form.

6.2 **"The Company Information System"** is any application, service or infrastructure that is used to store, process or transmit the Company Information.

6.3 **"Appropriate"** or **"Reasonable"** shall mean that which is consistent with this Policy, and the applicable procedures, standards and guidelines.

6.4 **"Confidential Information"** is any Company Information that, if disclosed to an unauthorized individual or third party, could result in substantial harm to the Company. Examples of Confidential Information include, but are not limited to:

6.4.1 Strategic marketing plans and Independent Representative Lists;

6.4.2 Proprietary research and development information;

6.4.3 Financial records, forecasts, minutes of Board of Directors meetings and material non-public information disclosure of which may affect an investment decision; and

6.4.4 Sensitive Personal Information, as defined in 6.9 below

6.5 **"Internal Information"** is any Company Information that the Company does not make available to the general public, but which does not qualify as Confidential Information.

6.6 **"Personal Information"** means any information accessed, collected, or used by the Company that identifies an individual, or can reasonably be used to identify an individual, whether directly or indirectly.

Examples of Personal Information include: name, mailing address, telephone or fax number, e-mail address, employee identification number, insurance policy or medical account number,

6.7 **"Sensitive Personal Information"** means Personal Information that requires an extra level of protection and a higher duty of care based on applicable law. Examples of Sensitive Personal

Information could include: credit card or bank account number, Government identification numbers, including Social Security numbers (SSN's), Social Insurance numbers, passport numbers, and driver's license numbers, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

6.8 **"Public Information"** is the Company Information that the Company:

6.8.1 Lawfully obtains from publicly available information or from federal, state or local government records that are lawfully made available to the general public; or

6.8.2 Intentionally makes available to the general public, including marketing materials, annual reports and public filings.

7.0 OWNERSHIP AND EXPECTATION OF PRIVACY

All information, digital or hardcopy, that is stored, processed, or transmitted using the Company Systems, is the property of the Company. Although Users may have individual passwords to access these Systems, the passwords belong to the Company. All information and communications using the Company-owned Systems and resources, including but not limited to, computer hardware, software, network, voice-mail, e-mail, instant messaging, web sites, social media sites used to conduct the Company business and/or containing the Company content, are the property of the Company and are accessible at all times by the Company.

Users should not store, process or transmit any personal information (e.g. personal passwords, financial account information, etc.) that they would not want the Company to view and/or retain. The Company additionally retains the right to remove from the Systems any material viewed as offensive, against this Policy or potentially illegal. If a User chooses to use the Company Systems to engage in personal communications, the User is doing so in full acknowledgement of the potential disclosure of these personal communications as a result of the Company monitoring and/or operations. Deletion or destruction of messages and communication will not provide confidentiality. Back-up copies of communications and messages are obtained and stored and may be reviewed and accessed when necessary.

To ensure compliance with policies, applicable laws and regulations, and employee safety, the Company reserves the right to monitor, inspect and/or search the Company Systems at any time. These Systems are subject to periodic unannounced inspections and may be conducted without User knowledge and/or permission.

8.0 INFORMATION MANAGEMENT

8.1 INFORMATION COLLECTION

The Company shall only collect information in a manner and scope that is consistent with applicable Company policies.

8.2 INFORMATION RETENTION

The Company shall limit the retention of Company Information in accordance with applicable Company records and information management policies and procedures and any applicable Legal Hold Notice (any notice issued by or at the direction of Legal advising the Company to retain and preserve particular categories of records indefinitely until Legal advises that retention is no longer required).

8.3 INFORMATION ACCESS

Management shall limit access to Company Information and Company Information Systems to those Company employees, contractors, and other third parties who require such access to perform their job duties or contractual obligations or engagement terms, as applicable.

8.4 INFORMATION STORAGE

The Company shall take reasonable steps to ensure that the Information under its control is stored in a manner that protects the security and confidentiality of such Information, based on the sensitivity of the Company Information and in accordance with this Policy, and the applicable procedures, standards and guidelines.

8.5 INFORMATION DISPOSAL

When Company Information in paper, electronic or other form is no longer required to be retained (including the Company Information stored on devices and media that are no longer to be retained), the Company Information must be properly disposed of in a manner that protects the security and confidentiality of such Information, based on the sensitivity of the Information and in accordance with this Security Policy, and the applicable procedures, standards and guidelines.

Paper records containing Confidential Information must be disposed of by shredding.

Electronic media (e.g., tape reels, floppy disks, CDs and DVDs, and hard disks, including hard disks on computers, printers and copiers) containing Confidential Information must be disposed of by shredding or degaussing the media as appropriate and consistent with the directives set forth in IT-004 Media Disposal.

9.0 RISK ASSESSMENT

9.1 ASSESSING SECURITY RISK

An integral part of the Company's approach to information security is the assessment of risk to the Company Information and Information Systems. The Director of Operations, as appropriate, shall incorporate such risks into the Company's Risk Assessment/ Compliance Program on a defined and periodic basis.

Users may be asked to facilitate the risk assessment process.

10.0 THIRD-PARTY ACCESS

10.1 GENERAL STATEMENT

The Company must (1) maintain appropriate security of the Company Information and the Company Information Systems that are accessed, processed, managed or otherwise handled by third parties, including service providers; and (2) select and retain third-party service providers that are capable of maintaining appropriate safeguards to protect the Company Information and the Company Information Systems, based on the sensitivity of the Company Information or the Company Information Systems.

10.2 WRITTEN AGREEMENT

Before providing a third party with access to the Company Information or the Company Information Systems that include Confidential Information, the Company must enter into a written agreement with the third party that requires the third party to implement appropriate procedures and safeguards based on the sensitivity of the Confidential Information to protect such the Company Information or the Company Information Systems in a manner consistent with the requirements of this Security Policy and its related procedures, standards and guidelines.

10.3 WRITTEN AGREEMENT CONTENTS

An agreement with a third party who will be provided with access to the Company Information or the Company Information Systems that include Confidential Information shall, as appropriate, include:

- an obligation to have, upon request, any material security issues identified by the Company remediated and the right to terminate the contract should the third party not remediate the issues within an appropriate timeframe;
- the right for the Company to audit or otherwise review the third party's security procedures and compliance with its obligation to appropriately protect such Company Information or the Company Information Systems;
- a limitation that the third party can only use such the Company Information or the Company Information Systems for the purpose of providing requested services to the Company; and
- an obligation that the third party notify the Company when the third party knows or has reason to believe that the Company Information or the Company Information System has been accessed or acquired by an unauthorized party or when otherwise required by law.

10.4 REVIEW

After providing a third party with access to (1) the Company Information Systems that contain Confidential Information or (2) Sensitive Personal Information (regardless of media or form), the Director of Operations shall periodically conduct a review to determine whether the third party is protecting such Information.

11.0 HUMAN RESOURCES SECURITY

11.1 PRIOR TO EMPLOYMENT

As appropriate and in accordance with relevant laws and regulations, the Director of Operations shall perform employee screening checks on all new employees that will be expected to have access to the Company Information.

11.2 DURING EMPLOYMENT

The Company employees who fail to comply with the information security requirements of this Security Policy, and the applicable procedures, standards and guidelines shall be subject to the Company's formal disciplinary process, including termination or disciplinary action.

11.3 TERMINATION OR CHANGE OF EMPLOYMENT

The Company shall have a formal process to ensure that all employment changes and transfers are processed and access controls and privileges can be removed or changed.

The Company shall ensure the return from terminated employees all Company Information, devices, media and other property in their possession upon termination of their employment.

The Director of Operations or his designee, working with the Company IT, shall remove or adjust as appropriate, the access rights of the employee upon a change in role and/or location.

12.0 PHYSICAL AND ENVIRONMENTAL SECURITY

The Director of Operations shall take reasonable steps to identify the risks that unauthorized individuals will gain access to the Company premises, Information, or Information Systems and will implement appropriate safeguards that are designed to limit those risks.

Users are to be educated to communicate physical or environmental risks that they feel are not accounted for or adequately controlled to the Director of Operations.

13.0 ELECTRONIC SECURITY

The Director of Operations shall take reasonable steps to identify the risks that unauthorized individuals will gain electronic access to Company Information and Information Systems and implement

appropriate safeguards that are designed to limit those risks in accordance with this Policy, and the applicable procedures, standards and guidelines.

Users should be educated to communicate risks of unauthorized access that they feel are not accounted for or adequately controlled to the Director of Operations.

14.0 INFORMATION SECURITY INCIDENT MANAGEMENT

14.1 REPORTING INFORMATION SECURITY EVENTS AND WEAKNESSES

The Company must have defined incident response procedures and train employees on how to report suspected or actual incidents in which an unauthorized party may have accessed the Company Information or Information Systems.

14.2 MANAGEMENT OF INFORMATION SECURITY INCIDENTS AND IMPROVEMENTS

Actual and suspected information security incidents shall be reported to and handled by the Company Director of Operations, with any necessary improvements made to this Security Policy and/or the Company Information Systems.

16.0 COMPLIANCE

The Company reserves the right to modify this Policy at any time and may use the Company e-mail system to distribute the notification of change. Users agree to be bound by all such modifications and revisions as a condition of continued Company Systems usage. Intentional and/or repeated non-compliance with this Policy will result in removal of System privileges and/or disciplinary action, up to and including termination of employment and/or potential civil or criminal liability. All Users must acknowledge and agree that they have read and understood this policy and must abide by it as a condition of the Company System usage. Users must also review and sign this Policy annually.

17.0 LOCATION OF OFFICIAL VERSIONS

The official version of this Security Policy and the related procedures, standards and guidelines issued pursuant to this Security Policy can be located in SharePoint.

18.0 EXCEPTIONS/APPROVALS

Requests for exceptions to the Policy must be submitted in writing to the Director of Operations or his designee. The Director of Operations or his designee will assess the appropriateness of the request, determine the risk of the exception, and if warranted, obtain approval from other members of senior management for Policy exception. All Policy exceptions will be recorded and reassessed at a minimum of once annually by the Director of Operations or his designee to ensure continued appropriateness. Exceptions may be revoked at any time, as deemed necessary by the Company, to ensure the continued protection of the Company Systems, data, and business interests.

19.0 CONTACT

Questions related to the interpretation or application of this Policy may be directed to the Director of Operations or his designee.

DOCUMENT CONTROL/REVISION HISTORY

Version	Date	Description of Change	Author
1.0	1/31/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

APPROVALS /SIGNOFF

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: User Account and Access Management	SOP No.: IT-001
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 4

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures for establishing, modifying and terminating user accounts and access for all systems, applications and data used by Audit Services U.S., LLC, ("the Company"). Adherence to this SOP protects the security, privacy, and integrity of systems and data stored, operated and maintained by the Company.

2.0 Scope

This SOP will apply to all users that are responsible for requesting and executing the creation, modification, and termination of user accounts and access rights for all systems, applications and data operated and maintained by the Company. This SOP applies not only to employees, but also guests, contractors, and anyone that will request, create, and/or provision user accounts and access rights.

3.0 Standards and Procedures

3.1 Account Management Requests

Account creation, modification and terminations requests must come from authorized members of management only. Requests received by those not authorized will be denied.

3.2 Account Creation

During initial account setup, certain checks and steps must be performed in order to ensure the integrity of the process.

- 3.2.1 Accounts must be created with proper authorization.
- 3.2.2 Accounts must be created for individuals only and never with the intention to be shared.
- 3.2.3 Accounts must be subject to the Company's Password Standard. No account specific exclusion criterion is to be selected. For example, no password expiration in Active Directory.

*If certain applications are not programmatically capable of supporting the minimum defined requirements above, a set of reasonable compensatory controls must be implemented to mitigate any additional risk incurred from the lack of the programmatic control. Any exceptions must be documented.

- 3.2.4 Account creations will be performed by the Director of Operations or an approved designee, such as a managed IT provider. Any designee must be appropriately trained in the security administration of the applicable system.
- 3.2.5 The Director of Operations is responsible for identifying and assigning the appropriate access required.
- 3.2.6 Accounts will have an e-mail address and mailbox assigned to that account unless otherwise instructed.
- 3.2.7 Where feasible, accounts are to be assigned to groups or roles. These groups or roles will facilitate distribution list addition and/or access right assignment. The groups or roles assigned are to be commensurate with the employee's roles and responsibilities.

Subject: User Account and Access Management	SOP No.: IT-001
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 4

- 3.2.8 Group or role memberships may be requested in a manner indicating that the memberships for the new employee will mimic those memberships of a prior or existing employee. If the rights are requested in this manner, the requestor must validate the access to be copied. Access assignments that are "one off", should be avoided if technically or operationally feasible.

3.4 Account Access Modification

Account access modifications must be properly authorized and have steps followed to ensure the integrity of the account management process and to reduce the risk of incorrect access right assignment. The following requirements must be followed when modifying user access rights:

- 3.4.1 Access change request must be communicated to and approved by the Director of Operations.

3.5 Account Termination

The timely termination of accounts is critical in maintaining the confidentiality, integrity, and availability of the systems and network resources used by the Company. The following requirements must be performed to facilitate the account termination process:

- 3.5.1 All termination requests are to formally documented and submitted to the appropriate security administrators for processing.
- 3.5.2 Upon receipt of the termination request, all access must be immediately suspended or suspended at the time specified in the request.
- 3.5.3 If the termination is considered to be a high risk termination (contentious), coordination with the Director of Operations must occur prior to the employee being notified of the termination. Once a time has been coordinated, the Director of Operations will execute the following steps while the employee is being informed of the termination:
- At management's discretion, a shut down of the employee's workstation must be conducted
 - All network, device, and application account access must be disabled
 - At management's discretion, a secure wipe of the company mobile phone will be issued
- 3.5.4 If the account is to remain active to facilitate usage of the account by another employee for the purpose of data extraction or e-mail monitoring, the password must be changed.

3.6 Account and Access Review

Account reviews are necessary to ensure that access remains relevant and accurate. The following will occur on a periodic basis:

- 3.6.1 Active Directory accounts will be reconciled yearly to ensure all active accounts belong to valid users.

Subject: User Account and Access Management	SOP No.: IT-001
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 4

- 3.6.2 Active Directory security and distribution group memberships will be validated yearly.
- 3.6.3 Network folder or Sharepoint folder access will be validated yearly.
- 3.6.4 Application access will be validated yearly.

Subject: User Account and Access Management	SOP No.: IT-001
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 4 of 4

Document Control/Revision History


Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Service Account Management	SOP No.: IT-002
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 2

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures for creating and maintaining service accounts used by Audit Services U.S., LLC ("the Company"). Adherence to this SOP protects the security, privacy, and data integrity of systems and data operated and maintained by the Company.

2.0 Scope

This SOP will apply to all service accounts that are created and maintained by the Company.

3.0 Standards and Procedures

- 3.0.1** Service accounts are not to be used as user accounts.
- 3.0.2** All service accounts must be unique and not shared by multiple applications.
- 3.0.3** Service account names must be reflective of the application it is authenticating.
- 3.0.4** Service account passwords must meet the following minimum standards:
 - Minimum length must be 15+ characters
 - Must contain a combination of upper and lower case letters, numbers, and special characters (i.e. ! @ #, etc)
- 3.0.5** Service account passwords must be changed at least once yearly.
- 3.0.6** Service accounts must be assigned the least privileges possible to execute only their intended function (e.g. read, write, execute, etc.).
- 3.0.7** Where operationally and technically feasible interactive logon should be disabled.
 - If interactive logon cannot be disabled the account must have the interactive logon access restricted to only the systems for which they are needed
- 3.0.8** Service accounts should never be assigned to an Active Directory privileged group (e.g. Domain Administrators, Enterprise Administrators) unless absolutely necessary for application operation.
- 3.0.9** If an employee with knowledge of the service account password leaves the Company, the password must be changed as soon as possible after termination.
- 3.0.10** If the password of a service account is suspected of being compromised it must be changed immediately.

Subject: Service Account Management	SOP No.: IT-002
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 2

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Privileged Account Management	SOP No.: IT-003
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures for creating and maintaining privileged accounts used by Audit Services U.S., LLC, ("the Company"). Privileged accounts can be defined as any account that is capable and authorized to perform administrative functions. Adherence to this SOP protects the security, privacy, and data integrity of systems and data operated and maintained by the Company.

2.0 Scope

This SOP will apply to all privileged accounts that are created and maintained by the Company for all system, network, and applications used and managed by the Company.

3.0 Standards and Procedures

Privileged accounts must only be assigned to personnel that are appropriately trained to use the account.

- 3.0.1** Privileged accounts must be strictly controlled and monitored.
- 3.0.2** Privileged accounts must be unique and not shared by multiple employees.
 - Note – Certain applications have a hard coded limitation of one administrator account. These applications will be considered exceptions to this requirement.
- 3.0.3** If an application has a default privileged account such as "administrator" or "sa", where technically and operationally feasible, that account is to be disabled or renamed.
- 3.0.4** Privileged accounts are never to be used as an employee's primary account.
- 3.0.5** Privileged accounts are only to be used to execute the functions needed and only for the duration necessary.
- 3.0.6** Privileged accounts are never to be used to access the web or read e-mails.
- 3.0.7** Privileged account passwords must meet the following minimum standards:
 - Minimum length must be 15+ characters
 - Must contain a combination of upper and lower case letters, numbers, and special characters (i.e. ! @ #, etc)
 - Must be changed every 180 days
- 3.0.8** If an employee with knowledge of a shared privileged account password leaves the Company, the password must be changed as soon as possible after termination
- 3.0.9** If the password of a privileged account is suspected of being compromised it must be changed immediately.

Subject: Privileged Account Management	SOP No.: IT-003
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

3.0.10 Privileged groups, whose members inherit privileged rights, must be reviewed on an annual basis to ensure access remains relevant and accurate. Examples of such groups are the Active Directory Domain Administrators, Enterprise Administrators, Administrators, and Schema Administrators groups.

Subject: Privileged Account Management	SOP No.: IT-003
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Media Disposal	SOP No.: IT-004
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 2

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which storage media must be disposed of to prevent the unauthorized disclosure of information. Adherence to this SOP protects the confidentiality of data created and stored by Audit Services U.S., LLC , (the "Company").

2.0 Scope

This SOP will apply to all media that is owned and/or leased by the Company and has been used in the creation and storage of Company data. This SOP will include internal and external hard drives, USB or flash drives, back-up tapes, and any other type of media where Company data may be stored.

3.0 Standards and Procedures

- 3.0.1** Systems or devices that contain company data, must have that data storage medium securely wiped or destroyed, prior to disposition.
- 3.0.2** Systems or devices, such as PC's, that are to be donated or gifted to employees, must have their storage media removed prior to the transfer of ownership
 - 3.0.2.1** The storage media that is removed can be reused for internal operations only or it must be destroyed.
 - 3.0.2.2** If Confidential Information existed on the removed electronic media and the media will be retained for later use, the Information must be removed.
- 3.0.3** Media will be destroyed only when it is has been deemed to be no longer functional or no longer capable of meeting the needs of the Company.
- 3.0.4** Media does not need to be destroyed at any specific interval; however, the media must be securely stored until destruction has been scheduled.
- 3.0.5** Specific to printers, copiers and fax machines, the hard drives must be sanitized prior to return to the leaser or disposed of.

Subject: Media Disposal	SOP No.: IT-004
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 2

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	4/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Patch Management	SOP No.: IT-005
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which patches will be identified, assessed, distributed and monitored. Adherence to this SOP protects the confidentiality, integrity, and availability of the systems and network resources owned and operated by Audit Services U.S. LLC, (the "Company").

2.0 Scope

This SOP will apply to all Company managed systems including desktops, laptops, servers, network devices, and applications that connect to the Company's network.

3.0 Policies and Procedures

3.1 Workstations and Servers

- 3.1.1 A server application must be maintained that is capable of distributing and reporting on the status of operating system and application updates.
- 3.1.2 Emergency patches that need to be applied must be approved by the Director of Operations.
- 3.1.3 Patch deployment status must be actively monitored to identify and rectify un-patched devices on a timely basis.
- 3.1.4 Patch management reports must be generated and supplied to the Director of Operations on a monthly basis. The report should clearly depict the status of all patched machines.

3.2 Types of Patches

- Servers/Computers – BIOS, Firmware, Drivers,
- Operating System – Service packs, patches, and feature packs,
- Application Software – Service packs, patches, feature packs,
- Anti-Virus – Data File/Virus Definition Update,
- Printers – Drivers/Firmware

Subject: Patch Management	SOP No.: IT-005
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

3.3 Schedule of patch deployment

Time	Description
Daily	<ul style="list-style-type: none"> • Anti-Virus and Spyware definitions must be configured to be installed automatically as released by vendor
Monthly	<ul style="list-style-type: none"> • Windows Operating System Patches after they are tested, and approved
Annually	<ul style="list-style-type: none"> • Printer (Drivers/Firmware) • Network Devices (Firmware, OS) • Workstation and Server Hardware (BIOS, Drivers)
Immediately	<ul style="list-style-type: none"> • Updates that should be applied immediately after they are tested and approved include: <ul style="list-style-type: none"> - Zero Day - Out of Band

Subject: Patch Management	SOP No.: IT-005
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Password Policy	SOP No.: IT-006
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 4

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of the entire corporate network. As such, all employees (including contractors and vendors with access to business systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system or network device used and managed by Audit Services U.S., LLC (the "Company"), has access to the Company network, or stores any non-public Company information.

4.0 Standards and Procedures

4.1 Password Construction

- 4.1.1** Each individual who will be provided access to a Company's Information System (a "User"), must be provided a unique User ID and a random unique initial password that is valid only for one log-on, at which point the User must be forced to choose another password.
- 4.1.2** A User must construct passwords that meet certain minimum security requirements.

4.1.2.1 Passwords

Must be at least eight characters in length (the length of passwords must be checked automatically at the time that Users construct or select them)

- 4.1.2.2** Must contain at least three out of the four following character sets:

- Numeric character (e.g., "1" or "4")
- Uppercase alpha character (e.g., "A" or "Z")
- Lowercase alpha character (e.g., "a" or "z")
- Special Character (e.g., "%" or "#")

- 4.1.2.3** Should not be easily guessable

- 4.1.2.4** Should not include proper names

- 4.1.2.5** Should not contain any portion of the User ID

Subject: Password Policy	SOP No.: IT-006
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 4

4.1.2.6 Should not use a basic sequence of characters that is then partially changed based on the date or some other predictable factor (e.g., using "X21JAN" in January or "X34FEB" in February or any combination with Company, such as "Company1234!")

4.1.2.7 Should not be identical or substantially similar to any of the User's previous four passwords.

4.1.2.8 Must be changed no later than 90 days.

4.1.2.9 Where technologically possible, all passwords traveling over any public or internal Company network must be encrypted.

4.2. Design of Password System User Interface

4.2.1 The display and printing of passwords must be masked, suppressed or otherwise obscured to limit unauthorized access or viewing of such information.

4.2.2 Vendor-supplied default passwords must be changed before any computer or communications software is used for Company business purposes.

4.2.3 The number of consecutive attempts to enter an incorrect password must be limited to ten (10) attempts, at which point the involved User ID must:

- Become suspended, until reset by a system administrator; or
- Become temporarily disabled for no less than fifteen (15) minutes; or
- Be reset via automated password reset tools

4.3. Password Transmission and Storage

4.3.1 If a security administrator of an application must transmit or otherwise communicate passwords that provide access to the Company computing environment, whether electronically or by mail, steps must be taken to safeguard such information from unauthorized access or use during transmission, including not transmitting passwords together with the associated User IDs.

4.3.2 The Company must take steps to prevent the retrieval of stored passwords from computer and communication systems, including by encrypting stored passwords.

4.3.3 Passwords may not be stored in plain text in:

- Readable form in batch files
- Automatic login scripts
- Software macros
- Terminal function keys
- Computers without access controls

4.3.4 If the requirements of 4.2.3 cannot be met, additional safeguards, such as private keys, should be implemented.

Subject: Password Policy	SOP No.: IT-006
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 4

4.4. Exceptions

If certain applications are not programmatically capable of supporting the minimum defined requirements above, a set of reasonable compensatory controls must be implemented to mitigate any additional risk incurred from the lack of the programmatic control.

Subject: Password Policy	SOP No.: IT-006
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 4 of 4

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Network Device Management and Security	SOP No.: IT-007
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which network devices will be managed and secured. Adherence to this SOP protects the confidentiality, integrity, and availability of the systems, data, and network resources owned and operated by Audit Services U.S., LLC (the "Company").

2.0 Scope

This SOP will apply to all Company managed network devices including firewalls, switches, routers, and wireless access points.

3.0 Policies and Procedures

3.1 General Standards for all Devices

The following are configuration standards that will apply to all devices based on industry defined best practice. This list is not all inclusive and where possible, additional security parameters will be added.

- 3.1.1** If Cisco devices are used, Enable secret must always be used and enable password is strictly forbidden.
- 3.1.2** Authentication, where possible, should occur through a radius type device that integrates with Windows Active Directory. Local logins are permitted; however, they must follow the standards defined for Account Management and Passwords.
- 3.1.3** Devices must be configured to explicitly deny telnet connections.
- 3.1.4** Devices must be managed through either secure shell ("SSH") or HTTPS.
- 3.1.5** SSH, HTTPS or Console sessions must time out after 10 minutes of inactivity.
- 3.1.6** If SNMP is not needed, it is to be disabled. If SNMP is used, it must be limited to RO. SNMP can never be configured to RW.
- 3.1.7** Where technically feasible, SNMP v3 will be used.
- 3.1.8** If SNMP v2 is used, default values must be changed.
 - 3.1.8.1** SNMPv2 values must:
 - Be at least 15 characters in length;
 - Contain upper and lower case letters, numbers and special characters;
 - Randomly generated and not related to the company name or contain dictionary type words.
- 3.1.9** Devices that are accessible through a management protocol from a source external to the network, must be restricted to an approved source IP address and/or require the establishment of a VPN.
- 3.1.10** Devices must be configured to synchronize with an authoritative time source.
- 3.1.11** Devices must be configured with the appropriate time zone.

Subject: Network Device Management and Security	SOP No.: IT-007
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

3.1.12 Publically accessible network devices configured with NTP must have an access control list placed on the service to prevent the device from becoming a public NTP server.

3.1.13 Logging with timestamps must be enabled.

3.2 Firewalls

3.2.1 All network packets entering or leaving a non-public Company network must first traverse a Company firewall, except for MPLS networks, leased lines, or other types of dedicated bandwidth from providers.

3.2.2 Firewalls must be configured to deny all incoming and egress traffic by default.

3.2.3 All ports that need to be opened to allow traffic flow must be subjected to the change management policy and procedures. All ports to be open must be verified to correspond to a business need and the potential risk of opening the port assessed to ensure acceptability.

- If the risk is deemed unacceptable, compensatory controls need to be investigated that will allow the business function to continue, but mitigate any additional risk.

3.2.4 Where feasible, traffic rules must be restricted to specific source, destination and protocol.

3.2.5 All rules must contain documentation in the configuration that specifies the purpose of the rule.

3.2.6 Firewall configurations must be reviewed on an annual basis by the Chief Compliance Officer and the IT group to ensure that the existing rules remain relevant and needed by the Company.

3.3 Switches

3.3.1 Ports that are unused must be disabled or physically restricted.

3.3.2 Switches are subject to an annual review to ensure accuracy of configurations, specifically as they relate to ACL's on VLAN's and general security protections.

Subject: Network Device Management and Security	SOP No.: IT-007
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Wireless Access Management	SOP No.: IT-008
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which wireless access must be managed and secured. Adherence to this SOP protects the confidentiality, integrity, and availability of the systems, data, and network resources owned and operated by Audit Services U.S., LLC, (the "Company").

2.0 Scope

This SOP will apply to all Company wireless access points and connections.

3.0 Standards and Procedures

3.1 Wireless Access

3.1.1 Corporate Wireless

Corporate Wireless is wireless access that provides connectivity to internal network resources on the private LAN.

3.1.1.1 All wireless Access Points / Base Stations connected to the network must be registered and approved by the Company.

3.1.1.2. All wireless LAN hardware implementations shall utilize Wi-Fi certified devices that are configured to use strong encryption protocols such as WPA-TKIP and AES.

3.1.1.3 The default SSID and administrative username / password shall be changed on all Access Points / Base Stations.

3.1.1.4 Device management shall follow the network device management standards.

3.1.2.5 All wireless access points that connect clients to the internal network (LAN) shall require users to provide unique authentication over secure channels and all data transmitted shall be encrypted with an approved encryption technology.

3.1.2 Guest Wireless

Visitors to the Company's primary office may be offered a guest wireless connection if requested.

3.1.2.1 The Guest wireless network must be logically or physically segmented from the Company internal corporate network.

3.1.2.2 The Guest wireless network is only permitted to allow internet bound traffic and access to select Company printers.

3.1.2.3 Access to the wireless network must require authentication and cannot be "open." Approved methods of communication are Pre-Shared Keys or Usernames and Passwords.

Subject: Wireless Access Management	SOP No.: IT-008
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

- If a Pre-Shared Key is used, it must be changed at a minimum of once annually.

3.1.2.4 A physical test of the segmentation must be conducted on an annual basis or whenever a change is made to a network device that may impact the segmentation.

Subject: Wireless Access Management	SOP No.: IT-008
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Physical Security	SOP No.: IT-009
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and standards by which IT assets are to be protected from unauthorized access, physical damage caused by accident or negligence, theft, and avoidable environmental hazards and natural disasters. This SOP will help ensure that Audit Services U.S., LLC, (the "Company") confidential information and technologies are not compromised and that IT assets and interests are protected from physical and environmental threats.

2.0 Scope

This SOP will apply to all personnel, including but not limited to IT Resources that access or require physical access to IT assets. All critical IT areas are subject to the Physical Security Standard.

3.0 Standard and Procedures

3.1 General Physical Security

- 3.1.1** Critical IT assets must be installed and maintained in areas that are secured and protected from unauthorized access.
- 3.1.2** All IT assets, including but not limited to servers and network hardware, that are of significant value or have a lifecycle, warranty and / or service level agreement must be recorded in an asset inventory.
- 3.1.3** Removable IT assets in critical IT areas, such as, tapes, cartridges, and storage drives must be securely stored.
- 3.1.4** With the exception to wet pipes used for fire suppression, no water, rain water, or drainage pipes should run within or above the critical IT areas so as to reduce the risk of flooding.

3.2 Physical Access Controls

- 3.2.1** Physical access to critical IT areas (e.g. primary and secondary data center) must be restricted to authorized personnel.
- 3.2.2** Critical IT areas must be secured with appropriate access controls, including but not limited to conventional key locks, key card systems, CCTV, and alarms. The appropriateness of access controls must be assessed based on key measures of the critical IT assets held in the critical IT areas including value, function, data contained, and network access.
- 3.2.3** Access to keys or other entry access systems including but not limited to electronic tags, swipe cards, and key codes for critical IT areas must be secured.
- 3.2.4** Unauthorized personnel and visitors who require access to critical IT areas must be monitored by authorized personnel.

3.3 Third Party Data Centers

Subject: Physical Security	SOP No.: IT-009
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

- 3.3.1** The company will assess and confirm the IT Controls of its third-party providers by reviewing the relevant SOC I or SOC II Type II reports as and when they are made available. If SOC I or SOC II Type II reports are not available, then the Company must perform reasonable due diligence to verify the appropriateness of the controls. Further the Company may perform or request IT controls based audits over third-party providers, as deemed necessary.

Subject: Physical Security	SOP No.: IT-009
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Vendor Access Management	SOP No.: IT-010
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 2

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which Vendors will be granted access to network resources. Adherence to this SOP protects the confidentiality, integrity, and availability of the systems, data, and network resources owned and operated by Audit Services U.S., LLC, (the "Company").

2.0 Scope

This SOP will apply to all Vendors that request access to internal network resources.

3.0 Standards and Procedures

3.1 Vendor Access

The following requirements are specific to the scenario where a physical account, firewall access rule, site to site VPN, or remote access agent must be created or installed to facilitate unattended access by a Vendor. This does not apply to Vendor access via technologies such as GoToMyPC or WebEx where an employee initiates the session.

At the discretion of the Company, any Vendor of any type can be asked to comply with all or a set of the following standards:

- 3.1.1** The Vendor must read and agree to the Company's acceptable usage policies.
- 3.1.2** The Vendor must sign a Company provided Non-Disclosure Agreement.
- 3.1.3** The Vendor must agree to:
 - 3.1.3.1** Restrict access to the Company's network to only those users that have a legitimate business need for access.
 - 3.1.3.2** Restrict access of those users to only the data and systems they have a business need to access.
 - 3.1.3.3** Provide the Company with names and any other relevant information about individuals that will have access to Company data and systems through the account and/or connection.
- 3.1.4** The Vendor user account will be subject to the defined Company password controls. The password controls that are implemented will depend on the type of account, standard user or administrative.
- 3.1.5** If the Vendor requires that a firewall rule is created to facilitate access, the Vendor must supply a source IP address or range and the destination ports required. The Company will not support a source address or port of type "ANY". If a range is supplied, the range must be verified to be owned by the Vendor.
- 3.1.6** If the Vendor requires a site to site VPN, the connection must comply with the SOP for "External Connection Management."

Subject: Vendor Access Management	SOP No.: IT-010
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 2

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

External Connection Management	SOP No.: IT-011
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 4

1.0 Purpose

This policy details Audit Services U.S., LLC (the "Company") standards for remote access management. The purpose of this policy is to specify the security standards required for such access, ensuring the integrity of data transmitted and received, and securing the pathways into the network.

2.0 Scope

The SOP applies to all connections to sites external to the Company's main site, and covers site-to-site VPN's, employee VPN's and direct telecom/WAN connections that are a part of the Company's infrastructure, including both sites requiring access to the Company's network (inbound) and sites where the Company connects to external resources (outbound).

3.0 Standards and Procedures

4.0 Site to Site VPN's

- 4.0.1 Site-to-site VPN's must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as AES 128. Direct connections, such as an MPLS connection, do not specifically require encryption unless the confidentiality of the data makes encryption necessary.
- 4.0.2 Site-to-site VPN's must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity of the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.
- 4.0.3 Pre-shared keys that are used in Site-to-site VPNs must meet the following security requirements.
 - 4.0.3.1 Be protected from unauthorized disclosure.
 - 4.0.3.2 Be a minimum of 32 characters in length.
 - 4.0.3.3 Contain a combination of upper and lower case letters, numbers and special characters.
 - 4.0.3.4 Be randomly generated.
 - 4.0.3.5 Changed as needed, but not to exceed once every three years.
- 4.0.4 If certificates are used instead of pre-shared keys, the certificates must expire and be regenerated after two years and contain at a minimum RSA 2048 bit keys and utilize the SHA2 Hashing algorithm.
- 4.0.5 The Company must manage its own VPN gateways, meaning that a third party must not provide and manage both sides of the site-to-site VPN, unless this arrangement is covered under an outsourcing agreement.

External Connection Management	SOP No.: IT-011
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 4

4.0.6 Site-to-site VPNs or WAN connections must adhere to the principle of least access and where technically or operationally feasible, limit the traffic flow to only the ports needed for business purposes.

4.0.7 Depending on the nature of the site-to-site VPN or WAN connection, the Company may use their discretion in the amount of logging and monitoring that is needed for the connection.

5.0 Employee Remote Access VPN's

5.1 SSL VPN's

5.1.1 SSL Certificates for SSL VPN's must be issued from a trusted root authority.

5.1.2 The certificate must contain at a minimum RSA 2048 bit keys.

5.1.3 Signature Hashing algorithm must be at a minimum SHA2.

5.1.4 SSL VPN must be implemented utilizing a RADIUS type authentication.

5.1.6 Access must be restricted to authorized users only.

- If integrated with Active Directory, the default "Administrator" account and Service accounts must be prohibited from authenticating via the VPN.

5.1.7 The session must terminate after 15 minutes of inactivity

5.1.8 Authorized VPN accounts must be recertified annually to ensure accuracy

5.2 IPSec Based VPN's

5.2.1 IPSec VPN's must utilize strong encryption to protect data during transmission. Encryption algorithms must meet or exceed current minimum industry standards, such as AES 128.

5.2.2 IPSec VPN's must utilize a strong password, pre-shared key, certificate, or other means of authentication to verify the identity of the remote entity. The strongest authentication method available must be used, which can vary from product-to-product.

5.2.3 Pre-shared keys that are used in IPSec VPNs must meet the following security requirements.

5.2.3.1 Be protected from unauthorized disclosure.

5.2.3.2 Be a minimum of 32 characters in length.

5.2.3.3 Contain a combination of upper and lower case letters, numbers and special characters.

External Connection Management	SOP No.: IT-011
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 4

5.2.3.4 Be randomly generated.

5.2.4 VPN must be implemented utilizing a RADIUS type authentication.

5.2.5 Access must be restricted to authorized users only.

- If integrated with Active Directory, the default "Administrator" account and Service accounts must be prohibited from authenticating via the VPN.

5.2.6 The session must terminate after 15 minutes of inactivity

5.2.7 Authorized VPN accounts must be recertified annually to ensure accuracy

External Connection Management	SOP No.: IT-011
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 4 of 4

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: General Network Security	SOP No.: IT-012
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 4

1.0 Purpose

This Standard Operating Procedure (SOP) describes the general standards and procedures by which the systems, network and data are protected at Audit Services U.S., LLC, (the "Company").

2.0 Scope

This SOP will apply to all Company managed systems including desktops, laptops, servers, network devices, and applications that connect to the Company's network.

3.0 Standards and Procedures

The Company implements a layered approach to security. The following practices and technologies are implemented:

4.0 Patch Management

Patch Management standards and procedures are defined in the Patch Management Policy

5.0 Antivirus

- 5.0.1** Up to date anti-virus scanning software must be deployed on all IT assets that connect to the Company's network domain.
- 5.0.2** Anti-virus server and/or workstation must be configured to:
 - Download anti-virus definition files on a daily basis and apply the definition files to IT assets connected to the network
 - Perform real time scanning of all IT assets connected to the network and send real time monitoring alerts to the Director of Operations and/or a suitable designee such as a managed IT Service provider upon detection of viruses
 - Execute an automated weekly virus scan of all local hard disks
 - Scans that are missed as a result of powered down machines must be scheduled to run on the next machine startup
- 5.0.3** The IT managed service provider must review daily anti-virus logs / real time alerts. Specific items that should be included and reviewed in the report are:
 - Infected Machine's
 - Machines with out of date antivirus updates or software
 - Machines with antivirus removed or disabled
- 5.0.4** IT assets that are infected with malware must be disconnected from the Company's network and scanned with approved Antivirus and Spyware tools. Infected files must be isolated and quarantined in a central location under management of the anti-virus console.
- 5.0.5** Users must be prohibited from altering anti-virus configuration, uninstalling anti-virus software or canceling anti-virus update cycles.

Subject: General Network Security	SOP No.: IT-012
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 4

5.0.6 New anti-virus and spyware software made available by the vendor must be reviewed within 30 days of its new release.

5.0.7 The IT managed service provider is to provide the Director of Operations on a monthly basis an executive summary regarding the status of the antivirus protection on all workstation and servers.

6.1 Firewalls

6.1.1 All servers and workstations must be configured with a firewall.

6.1.2 Inbound traffic must be restricted to authorized ports only. Authorized ports are ports that have a business justification. Outbound restrictions are optional.

6.1.3 Users must be prohibited from disabling the firewall.

7.2 Local Accounts

7.2.1 Network authentication must be disabled for all local accounts.

7.2.2 The local "Administrator" account must have a password that conforms to the complexity of the privileged account password standard.

7.2.3 Should an employee with knowledge of the password leave, the password must be changed as soon as possible after termination

7.2.4 The local "Administrator" account password must be different between servers and workstations.

7.2.5 Unless authorized by the Director of Operations, employees are prohibited from being granted permanent membership in the local "Administrators" group. Temporary membership is authorized to facilitate troubleshooting procedures; however, membership must be immediately removed upon completion.

8.0 E-mail Scanning

8.0.1 All inbound and outbound e-mails must be scanned by an e-mail filtering system that is capable of detecting SPAM and/or malicious content (i.e. malware, virus, etc).

8.0.2 E-Mails containing known malware or any executable type attachments (.exe, .vbs, .bat) are strictly prohibited and must be quarantined and/or deleted by the scanning device. If quarantined, only IT can be provided access to review the e-mail. The end user must not be provided the option of accessing and/or releasing the e-mail with the attachment.

8.0.3 E-Mails originating from outside the Company e-mail domain that contain spoofed internal addresses must be deleted or quarantined.

9.0 Session Timeouts

IT assets that support timeout configuration settings including desktops, Remote Desktop (RDP), and Virtual Private Network (VPN) must be timed out after 15 minutes of non-usage (e.g., password-protected screensaver, automatic log-outs).

Subject: General Network Security	SOP No.: IT-012
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 4

10.0 Windows Monitoring

10.0.1 Windows Audit Policies must be enabled on critical IT assets for audit policies including but not limited to:

- Account logon events (Success, Failure)
- Logon events (Success, Failure)
- Account Management (Success, Failure)
- Directory Service Access (Success, Failure)
- Policy Change (Success, Failure)
- Privilege Use (Success, Failure)
- File level access must be audited and monitored on any repositories that contain protected personal information.

On an annual basis, the Director of Operations in conjunction with the IT managed service provider must review Group Policy settings are still accurate and relevant.

11.0 Encryption

All laptops and removable media supplied to employees by the company must be encrypted using industry standard encryption technology.

12.0 Removable Media

Removable media not authorized, supplied and encrypted by the Company is strictly prohibited.

13.0 Application Monitoring

Applications that contain protected personal information must have all relevant security events audited and monitored. Such events may include:

- Account logon events (Success, Failure)
- Logon events (Success, Failure)
- Account Management (Success, Failure)
- Policy Change (Success, Failure)
- Privilege Use (Success, Failure)
- Record viewing, editing and printing. (Success, Failure)

Procedures must be defined to review this audit events on a periodic basis.

Alerts should be defined for key security events, such as account lockouts.

Subject: General Network Security	SOP No.: IT-012
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 4 of 4

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Change Management	SOP No.: IT-013
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 2

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and procedures by which changes to key information systems and devices must be approved, tested, and recorded.

2.0 Scope

This SOP will apply to all critical information systems, applications and network resources owned and operated by Audit Services U.S. LLC, (the "Company").

3.1 Standard and Procedures

- All changes that may potentially impact the confidentiality, integrity or availability of the network must be communicated to and approved by the Director of Operations.
- Were applicable, a backup of the application, data and/or network device must be taken prior to performing the change.
- Were applicable, a recovery plan must be established prior to the implementation of the change.
- A log of all significant changes must be maintained.

Subject: Change Management	SOP No.: IT-013
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 2

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in forces	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Subject: Backup Management Policy	SOP No.: IT-014
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 1 of 3

1.0 Purpose

This Standard Operating Procedure (SOP) describes the policies and standards by which Backup procedures for Audit Services U.S. LLC, (the "Company"), for both Data and Configurations is maintained. This policy encompasses the methods, data types, frequency, and roles used to maintain the integrity and availability of the Company information.

2.0 Scope

This SOP will apply to all backup and recovery of all mission critical applications and equipment configuration.

3.0 Standard and Procedures

3.1 Role and Responsibilities

- 3.1.1** The managed IT service providers must ensure that the backup of data and configurations occurs according to schedule.
- 3.1.2** All failed and unsuccessful back-ups shall be remediated by the appropriate managed IT service provider.
- 3.1.3** Enforcement of these procedures is the responsibility of the Director of Operations.

3.2 Back-up Retention and Frequency

Backup Retention and Scheduling for Data and Configurations will vary based on the type of data being backed up and the tool being used.

- 3.2.1** All systems must be backed up at a minimum of once daily.
- 3.2.2** Retention requirements must be defined to match the Company's document retention schedule.

3.3 Data Back-up Monitoring

- 3.3.1** The managed IT service providers must review the backup status on a daily basis to confirm successful completion of the backups.
- 3.3.2** The backup applications must be configured to alert on back-up failures upon completion of the back-up jobs. If unknown back-up failures occur, they must be reviewed upon alert and appropriate troubleshooting procedures performed.
- 3.3.3** Data back-up logs must be retained for a period of one year.
- 3.3.4** On a weekly basis, the managed IT service provider is to provide the Director of Operations an executive summary report of the backup status for the prior week.

Subject: Backup Management Policy	SOP No.: IT-014
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 2 of 3

3.4 Data Back-Up Verification and Restoration

- 3.4.1** On an annual basis, critical applications must be restored to an alternate location or virtual test environment to verify the readability of the back-up media. Reconciliations are to be performed by appropriate personal to ensure the accuracy of the restored data.
- 3.4.2** On an annual basis, the backup software configuration is to be reconciled against the application vendor and the Company's backup requirements to ensure all necessary data is included in the backup routines.
- 3.4.3** Recovery of lost data "owned" and "requested" by the user must be performed in accordance with the restoration procedures. Recovery of lost data "not owned" by the user must be approved by the Director of Operations (e.g., mailbox recovery of terminated employees).

Subject: Backup Management Policy	SOP No.: IT-014
	Version No.: 1.3
	Effective Date: 06/30/2022
	Page 3 of 3

Document Control/Revision History

Version	Date	Description of Change	Author
1.0	01/23/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

Approvals /Signoff

The information security policies identified here-in are based on industry standards that document accepted good security practices. I approve this information security policy and expect the policies to be implemented consistently throughout the Company.

Employee Name: J Matthew Thornton

Title: Managing Member, Director of Operations

Signature:  Date: 06/30/2022

Audit Services U.S., LLC

Employee Acceptable Use Policy

Table of Contents

1.0 PURPOSE AND SCOPE	3
2.0 APPLICABILITY	3
3.0 BACKGROUND	3
4.0 RESPONSIBILITIES	3
5.0 DEFINITIONS	3
6.0 OWNERSHIP AND EXPECTATION OF PRIVACY.....	4
7.0 USER ACCEPTABLE USE AND RESPONSIBILITIES	5
7.1 ACCEPTABLE USE	5
7.2 UNACCEPTABLE USE	5
7.3 EXCHANGE OF INFORMATION	7
7.4 ANTI-VIRUS.....	7
7.5 DOCUMENT AND DATA STORAGE.....	8
7.6 PASSWORD POLICY.....	8
7.7 USE OF PERSONAL DEVICE POLICY.....	9
7.8 PHYSICAL SECURITY.....	9
7.9 REMOVABLE MEDIA.....	10
7.10 THEFT OR LOSS OF DATA OR EQUIPMENT.....	10
7.11 PROTECTION OF CLIENT SENSITIVE INFORMATION.....	10
8.0 COMPLIANCE	10
9.0 LOCATION OF OFFICIAL VERSIONS	10
10.0 EXCEPTIONS/APPROVALS	11
11.0 CONTACT	11
DOCUMENT CONTROL/REVISION HISTORY	11
APPROVALS /SIGNOFF	11

1.0 PURPOSE AND SCOPE

The purpose of this policy is to outline the acceptable use of computer equipment at Audit Services, US, LLC. (the "Company"). These rules are in place to protect the employee and the Company. Inappropriate use exposes the Company to risks including virus attacks, compromise of network systems and services, and legal issues. This policy is designed to provide a framework of acceptable employee usage.

2.0 APPLICABILITY

This Security Policy applies to all Supervised Persons, contractors, consultants, temporaries, per diems, and other workers at the Company. These policies apply to all equipment, software, data, and systems that are owned or leased by the Company.

If the Company is subject to a law that establishes a higher or more detailed standard than provided in this Security Policy, the Company must comply with such law.

3.0 BACKGROUND

This Security Policy is designed to protect the confidentiality, integrity, and availability of the Company Information and the Company Information Systems:

Confidentiality: ensuring that the Company Information and the Company Information Systems are secure and accessible only to those authorized to have access;

Integrity: safeguarding the accuracy and completeness of the Company Information, the Company Information Systems, and processing methods;

Availability: ensuring that authorized users have access to the Company Information and the Company Information Systems when required.

4.0 RESPONSIBILITIES

Users ("User" is defined as all Supervised Persons of the Company and any other person to whom access to the Company systems is granted.) are responsible for reading and complying with the Company IT regulations, specifically

Each User is responsible for:

- Being aware of the contents of this policy and the related procedures, standards and guidelines that are applicable to him or her ("Applicable Procedures");
- Ensuring that his or her actions comply with the requirements of this Security Policy and the applicable procedures, standards and guidelines;
- Completing any required training regarding this Security Policy and its Applicable Procedures, as administered by the Director of Operations or his designee;
- Asking questions of the Director of Operations when uncertain of how to comply with the requirements of this Security Policy and the applicable procedures, standards and guidelines; and
- Reporting any violations to the Director of Operations or his designee.
- Certifying to his or her understanding of this Security Policy and the applicable procedures, standards and guidelines through the means used by the Company for such certification.

5.0 DEFINITIONS

5.1 "The Company Information" is any information that is collected, used or maintained by the Company regardless of form.

5.2 **"The Company Information System"** is any application, service or infrastructure that is used to store, process or transmit the Company Information.

5.3 **"Appropriate"** or **"Reasonable"** shall mean that which is consistent with this Policy, and the applicable procedures, standards and guidelines.

5.4 **"Confidential Information"** is any Company Information that, if disclosed to an unauthorized individual or third party, could result in substantial harm to the Company. Examples of Confidential Information include, but are not limited to:

5.4.1 Strategic marketing plans and Independent Representative Lists;

5.4.2 Proprietary research and development information;

5.4.3 Financial records, forecasts, minutes of Board of Directors meetings and material non-public information disclosure of which may affect an investment decision; and

5.4.4 Sensitive Personal Information, as defined in 6.9 below

5.5 **"Internal Information"** is any Company Information that the Company does not make available to the general public, but which does not qualify as Confidential Information.

5.6 **"Personal Information"** means any information accessed, collected, or used by the Company that identifies an individual, or can reasonably be used to identify an individual, whether directly or indirectly.

Examples of Personal Information include: name, mailing address, telephone or fax number, e-mail address, employee identification number, insurance policy or medical account number,

5.7 **"Sensitive Personal Information"** means Personal Information that requires an extra level of protection and a higher duty of care based on applicable law. Examples of Sensitive Personal Information could include: credit card or bank account number, Government identification numbers, including Social Security numbers (SSN's), Social Insurance numbers, passport numbers, and driver's license numbers, information on medical or health conditions, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, sexual preferences, or information related to offenses or criminal convictions.

5.8 **"Public Information"** is the Company Information that the Company:

5.8.1 Lawfully obtains from publicly available information or from federal, state or local government records that are lawfully made available to the general public; or

5.8.2 Intentionally makes available to the general public, including marketing materials, annual reports and public filings.

6.0 OWNERSHIP AND EXPECTATION OF PRIVACY

All information, digital or hardcopy, that is stored, processed, or transmitted using the Company Systems, is the property of the Company. Although Users may have individual passwords to access these Systems, the passwords belong to the Company. All information and communications using the Company-owned Systems and resources, including but not limited to, computer hardware, software, network, voice-mail, e-mail, instant messaging, web sites, social media sites used to conduct the Company business and/or containing the Company content, are the property of the Company and are accessible at all times by the Company.

Users should not store, process or transmit any personal information (e.g. personal passwords, financial account information, etc.) that they would not want the Company to view and/or retain. The Company additionally retains the right to remove from the Systems any material viewed as offensive, against this Policy or potentially illegal. If a User chooses to use the Company Systems to engage in personal communications, the User is doing so in full acknowledgement of the potential disclosure of these personal communications as a result of the Company monitoring and/or operations. Deletion or destruction of messages and communication will not provide confidentiality. Back-up copies of

communications and messages are obtained and stored and may be reviewed and accessed when necessary.

To ensure compliance with policies, applicable laws and regulations, and employee safety, the Company reserves the right to monitor, inspect and/or search the Company Systems at any time. These Systems are subject to periodic unannounced inspections and may be conducted without User knowledge and/or permission.

7.0 USER ACCEPTABLE USE AND RESPONSIBILITIES

While it is recognized that incidental and occasional personal use of the Company Systems may occur, personal use must not interfere or conflict with the Company business and the User's responsibilities to the Company and its clients.

7.1 ACCEPTABLE USE

- Users are responsible for exercising good judgment in personal use. Should Users have any questions, Users should consult the Director of Operations or his designee.
- Users must keep passwords secure and may not share accounts. Authorized Users are responsible for the security of their passwords and accounts
- All laptops and workstations should be password protected when left unattended
- Users must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.
- All electronic communications for Company business must be conducted on the Company e-mail system.
- Users that wish to accommodate client or guest requests for internet access at the Company's one of our office locations must use the guest wireless network. Do not instruct the guest to just "plug-in" to a network connection.

7.2 UNACCEPTABLE USE

The following activities are, in general, prohibited. Users may be exempted from these restrictions during the course of their legitimate job responsibilities based on circumstances (e.g. IT may have a need to disable the network access of a host if that host is disrupting production services). (Exemptions may be provided by Director of Operations or his designee.)

No User may engage in any activity that is illegal or prohibited under local, state, federal or international law or regulation while utilizing the Company owned resources.

The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are prohibited:

- Violating the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by the Company.
- Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The Director of Operations or his designee should be consulted prior to export of any material that is in question.
- Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

- Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.
- Using the Company computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the User's local jurisdiction.
- Making fraudulent offers of products, items, or services originating from any Company account.
- Making statements about warranty, expressly or implied, unless it is a part of the normal job duties.
- Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.
- Port scanning or security scanning is expressly prohibited unless prior approval from the Director of Operations or his designee.
- Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.
- Circumventing user authentication or security of any host, network or account (i.e. disabling or interfering with the installation or distribution of security patches, antivirus definitions, etc.).
- Attempt to change the Company networks, install modem lines, setup connections to external networks or ISPs or attempt any other alteration to the Company networks.
- Connecting routers, switches and wireless access points (e.g. wireless routers) to the internal network.
- Interfering with or denying service to any User other than the employee's host (for example, denial of service attack).
- Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a User's terminal session, via any means, locally or via the Internet/Intranet/Extranet.
- Although aesthetic personalization is allowed to such areas as the desktop wallpaper, screensaver, etc., the User must exercise professional judgment in the selection of these customizations and cannot display anything that may be considered offensive or insulting. Strictly prohibited, are any images or content that are derogatory, sexual in nature, depict illegal activities or illicit substances, or are offensive to an individual's religious beliefs, gender, sexual orientation, ethnicity, disability, or political views.
- Providing information about, or lists of, Company users to parties outside the Company, unless part of normal job duties, such as employment verification by Human Resources or communications with payroll administrator.

E-mail and Communications Activities

The following activities are prohibited:

- Conducting Company business communications using personal e-mail systems is strictly prohibited. (Social media, posts, or blogs are not approved communication systems).
- The use of any file storage/transfer website or application not explicitly authorized and/or provided by the Company for the transfer, storage or sharing of client and the Company

data is strictly prohibited. Such websites forbidden include but are not limited to Drop Box, SkyDrive, Google Docs, File Convoy, etc.

- Users may use a secure file storage/transfer website that is provided by the requesting party to assist with data transmission
- Sending unsolicited e-mail messages, that are not business related including the sending of "junk mail".
- Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.
- Unauthorized use of e-mail header information
- Solicitation of e-mail for any other e-mail address, other than that of the poster's account, with the intent to harass or to collect replies.
- Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.
- Broadcast Messages (i.e. sending e-mail to all employees) is strictly limited to the following: IT, Human Resources and Senior Management.

7.3 EXCHANGE OF INFORMATION

All Company Users shall take reasonable steps to ensure that the transmission of the Company Information within the organization or to third parties is secured from unauthorized access or disclosure in accordance with this policy, and the applicable procedures, standards and guidelines, and based on the sensitivity of the Company Information.

The following types of information shall not be communicated electronically outside of the Company over a public network (wired or wireless) (other than by fax or telephone) unless the Company Information is encrypted:

- Confidential Information, the disclosure of which will directly cause damage to the Company market share and/or market capitalization, and
- Sensitive Personal Information.

7.4 ANTI-VIRUS

Antivirus plays a critical role in maintaining the confidentiality, integrity, and availability of the Company information and network resources.

Currently, the Company deploys anti-virus agents for all Windows OS workstations and servers.

- The latest DAT file will be automatically downloaded and installed to each client on a daily basis to ensure the latest virus definitions are available.
- Any activity intended to create and/or distribute malicious programs onto the Company network (e.g. viruses, worms, Trojan horses, e-mail bombs, etc.) is strictly prohibited.

Users should:

- Never open any files or macros attached to an e-mail from an unknown, suspicious or untrustworthy source. Delete these attachments immediately, then "double delete" them by emptying your Trash.
- Attempt to circumvent the antivirus functionality by disabling or uninstalling the application.
- Delete spam, chain, and other junk e-mail without forwarding.
- Never download files from unknown or suspicious sources.
- Avoid direct disk sharing with read/write access.

- Save critical data and system configurations on a regular basis and store the data in a safe place (network drive location).
- If a User receives what he/she believes to be a virus, or suspects that a computer is infected with a virus, he/she must report such incident to the Director of Operations, his designee or the IT service group immediately. Report the following information (if known): virus name, extent of infection, source of virus, and potential recipients of infected material.
- No User should attempt to destroy or remove a virus, or any evidence of that virus, without direction from the Director of Operations or his designee.
- Any virus-infected computer will be removed from the network until it is verified as virus-free.

7.5 DOCUMENT AND DATA STORAGE

The Company maintains responsibility for the back-up of files maintained in designated network locations. When working remotely without the Company network connectivity, it is the responsibility of the User to perform all necessary back-ups to safeguard the Company related data.

If a User chooses to store files locally without any associated backup or network copy, the User is doing so at the risk of data loss or corruption in the event of software or hardware failure.

The Company at all times reserves the right to delete personal files from their Systems and storage locations, both local and on the network. The storage of non-business related media files (e.g., audio, graphic and video files), entire programs, games and back-up copies of computer hard drives are strictly prohibited and subject to deletion without notice.

7.6 PASSWORD POLICY

Passwords are in common use, they are easy to create and have been the standard for User authentication for a very long time. That means they are susceptible to attack and Users must exercise care when using passwords.

7.6.1 General Password Policy

All passwords used for internal Company systems or third party internet accounts, where technically feasible, will be configured to require the following password parameters:

- **First use:** The initial password assigned to Users for access to any of the Company systems and applications must be changed on initial login. If the password is not required to be changed on first use, contact the IT Support immediately to have the issue corrected.
- **Password aging:** All Company computer users must change his or her password at least every 90 days. Attempts to login using an expired password will not succeed.
- **Reuse of old passwords:** New passwords must be different from the four prior passwords.
- **Account Lockout:** Entry of an incorrect password after ten successive unsuccessful attempts will result in the account being locked for usage. Once the account is locked, login attempts will be unsuccessful for a period of 15 minutes or until Administrator intervention.
- **Password Strength:** To qualify, passwords selected must meet to the following strength requirements:
 1. Be made up of at least eight characters
 2. Not be a word found in the dictionary or be among passwords that are easy to guess, such as birthdays, names of pets, user login name, first name, last name,

company name, phone extension, or any other easily identifiable words and phrases like 'goyankees'.

3. Contains AT LEAST THREE out of the four character types.

- Upper-case alphabet characters (A...Z)
- Lower-case alphabet characters (a...z)
- Numbers (0...9)
- Non-alphanumeric characters (e.g., !\$#@%\$)

7.6.2 Password Protection Policy

- Do not share the Company passwords with anyone, including IT Department staff, administrative assistants, secretaries and family members. All passwords are to be treated as sensitive, confidential Company information.
- Do not write down or store passwords on-line without encryption.
- Do not reveal a password in e-mail, chat, or other electronic communication.
- Do not speak about a password in front of others.
- Do not hint at the format of a password. (e.g., "my family name")
- Do not reveal a password on questionnaires or security forms.
- Always decline the use of the "Remember Password" feature of applications. (e.g., Google, Internet Explorer, etc.)

If an account or password compromise is suspected, report the incident to the Director of Operations.

7.7 USE OF PERSONAL DEVICE POLICY

The use of personal employee devices such as Laptop and PC's are strictly prohibited from accessing Company data. While employees are permitted to work remotely when not in the physical office, they must do so on Company owned and secured equipment.

The Company permits the use of Smartphone/Cellular/PDA devices as means for business e-mail communications only if they go through the Company's e-mail system. These devices are required to be registered on the Company's corporate e-mail system and are controlled and safeguarded via the Company's centrally administered email system. Employees must read and agree to a separate Mobile Device Policy, before authorization to connect the phone is granted.

All electronic communications for the Company's business must be conducted on the Company e-mail system. The use of personal e-mail systems or text messaging is strictly prohibited.

Company data is never to be saved locally to a personally owned device.

7.8 PHYSICAL SECURITY

This policy is designed to deny access to unauthorized personnel who attempt to physically access a building, facility, resource, or stored information. It also serves to protect personnel, hardware, programs, networks, and data from physical circumstances and events that could cause serious losses or damage. This policy applies to Users including all personnel affiliated with third parties.

- All Users shall follow a clean desk policy. As such, papers that are sensitive in nature should never be left on the desk and unattended.
- All IT equipment and information that require access protection should be placed in secure physical areas. Secure areas should have suitable access control to ensure that only authorized personnel have access.
- Users are responsible for the Company-owned laptops and portable storage devices when taken outside of the Company office space. All laptops or portable storage devices should never be left unattended when removed from the office. Laptops should never be left unattended,

even for a few minutes, particularly in an unattended non-Company office or on the train. If left in a car, laptops should be locked in the trunk out of sight, not on the seat.

7.9 REMOVABLE MEDIA

Personal (non-company-owned) storage devices represent a serious threat to data security and are expressly prohibited from being connected to the Company's systems and network and used in the storage of Company data. Examples of this are: USB drives, flash storage, media players, etc.

Encrypted storage media supplied by the Company is allowed to employees that have a business need and have been authorized by the Director of Operations or his designee.

7.10 THEFT OR LOSS OF DATA OR EQUIPMENT

Users must immediately report the theft, loss or erroneous disclosure of any item containing Company and/or sensitive information. This is critical to ensure that the Company can take the appropriate actions to mitigate the risk of unauthorized information disclosure and if necessary alert the affected employees, clients, and/or necessary State and/or Federal agencies. The loss of such items include, but are not limited to:

- Equipment such as laptops and other mobile devices.
- Media such as CDs or flash drives.
- E-mails, faxes and other transmissions sent to the wrong persons.
- Paper documents, such as client files or confirmation letters.

7.11 PROTECTION OF CLIENT SENSITIVE INFORMATION

Sensitive Personal Information, such as client Social Security Numbers or account numbers must receive the highest degree of security and care when being used, stored or transmitted.

Client sensitive personal information must:

- never be e-mailed or removed from the designated secured locations in an unencrypted format.
- never be left exposed in plain sight or left in an unsecured location if printed.
- be securely destroyed electronically when media is disposed of.
- be securely shredded if in paper format.
- never be shared with any party not authorized or privy to the information.

8.0 COMPLIANCE

The Company reserves the right to modify this Policy at any time and may use the Company e-mail system to distribute the notification of change. Users agree to be bound by all such modifications and revisions as a condition of continued Company Systems usage. Intentional and/or repeated non-compliance with this Policy will result in removal of System privileges and/or disciplinary action, up to and including termination of employment and/or potential civil or criminal liability. All Users must acknowledge and agree that they have read and understood this policy and must abide by it as a condition of the Company System usage. Users must also review and sign this Policy annually.

9.0 LOCATION OF OFFICIAL VERSIONS

The official version of this Security Policy and the related procedures, standards and guidelines issued pursuant to this Security Policy can be in the Network Directory.

10.0 EXCEPTIONS/APPROVALS

Requests for exceptions to the Policy must be submitted in writing to the Director of Operations or his designee. The Director of Operations or his designee will assess the appropriateness of the request, determine the risk of the exception, and if warranted, obtain approval from other members of senior management for Policy exception. All Policy exceptions will be recorded and reassessed at a minimum of once annually by the Director of Operations or his designee to ensure continued appropriateness. Exceptions may be revoked at any time, as deemed necessary by the Company, to ensure the continued protection of the Company Systems, data, and business interests.

11.0 CONTACT

Questions related to the interpretation or application of this Policy may be directed to the Director of Operations or his designee.

DOCUMENT CONTROL/REVISION HISTORY

Version	Date	Description of Change	Author
1.0	12/20/2018	Draft policy published	Director of Operations
1.1	04/11/2018	Policy published and in force	Director of Operations
1.2	01/15/2021	Policy reviewed, published and in force	Director of Operations
1.3	06/30/2022	Policy reviewed, published and in force	Director of Operations

APPROVALS /SIGNOFF

I have read this information security policy and understand what is required of me to protect the Company's network, systems and data. I agree to abide by this policy and understand failure to do so could result in formal disciplinary action, including termination of employment.

Employee Name: _____

Signature: _____ Date: _____

MOBILE DEVICE POLICY

Audit Services U.S. LLC, (the "Company") grants its employees the privilege of using a personal smartphone or tablet to access Company e-mail for their convenience. Employees are permitted to connect these devices to the guest Wi-Fi network only while at work. At no time is a personal device of any kind to be connected directly to the Company computers or the internal network. The Company reserves the right to revoke this privilege if the user does not abide by the policies and procedures outlined below.

This policy is intended to protect the security and integrity of the Company's data and technology infrastructure. Limited exceptions to the security provisions of this policy may occur but must first be approved by the Director of Operations. The Company's e-mail messaging systems are not private and may be monitored by the Company.

Company employees must agree to the terms and conditions set forth in this policy in order to connect their devices to Company resources.

- In order to prevent unauthorized access, devices must be password protected using the features of the device. This may include a password or fingerprint.
 - Passwords are not to be shared with any person under any circumstance. If an employee has reason to believe his or her password has been compromised, then the password must be changed immediately.
 - Passwords are to consist of the following:
 - 5 character minimum length.
 - Consist of a letter, number and special character.
- The device must lock itself if idle for five minutes.
- If ten failed password attempts occur in succession, the device will automatically wipe itself and reset to factory defaults.
- Lost or stolen devices must be reported to the company within 24 hours. Employees are responsible for notifying their mobile carrier immediately upon loss of a device.
- The company reserves the right to disconnect devices or disable services without notification.
- The employee's device may be remotely wiped if
 - the device is lost,
 - the employee terminates his or her employment,
 - IT detects a data or policy breach, a virus or similar threat to the security of the company's data and technology infrastructure.
- While IT will take every precaution to prevent the employee's personal data from being lost in the event it must remote wipe a device, it is the employee's responsibility to take additional precautions, such as backing up email, contacts, etc.
- Not all smartphones and tablet models are capable of accessing company resources.
- Rooted (Android) or jailbroken (iOS) devices are prohibited from accessing Company resources.
- Employees' access to company data is limited based on user profiles defined by IT and automatically enforced.
- The Company prohibits the use of e-mail messaging systems that is in any way offensive.
- All acceptable use policies with regards to e-mail and privacy apply to the mobile device.

APPROVALS /SIGNOFF

I have read this information security policy and understand what is required of me to protect the Company's network, systems and data. I agree to abide by this policy and understand failure to do so could result in formal disciplinary action, including termination of employment.

Employee Name: _____

Signature: _____ Date: _____

ASUS EXHIBIT E

BHDS
Certification and
SOC Reports



Blue Hill Data Services Compliance and Certifications

Blue Hill is SOC 2 Type 2 (SSAE 18) Compliant

By successfully completing an annual SOC 2 Type 2 examination, by a third-party auditor, Blue Hill gains assurance for its clients for the controls it has put in place at its hosted data center facility in Pearl River, NY. This examination validates that the policies and procedures Blue Hill has in place comply with important SOC 2 Type 2 (SSAE 18) standards regarding security, availability, processing integrity, confidentiality, or privacy, relevant to a client's confidential and critical data. SOC 2 also aligns with international standards and includes a written assertion from management on the design and operating effectiveness of the data center controls.



~ SOC 2 Type 2 Compliant ~

SOC 2 Type 2 examination reports on Controls at a Service Organization in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 18, validating and reporting on the controls in place for Data Center Hosting Services. Blue Hill maintains the policies and procedures and the design and operating effectiveness to comply with these regulatory requirements.

Blue Hill is SOC 1 Type 2 (SSAE 18) Compliant

By successfully completing an annual SOC 1 Type 2 examination, by a third-party auditor, Blue Hill gains assurance for its clients for the controls it has put in place at its hosted data center facility in Pearl River, NY. This examination validates that the policies and procedures Blue Hill has in place comply with important SOC 1 (SSAE 18) standards regarding business process and information technology relevant to user entities' internal control over financial reporting. SOC 1 Type 2 also aligns with international standards and includes a written assertion from management on the design and operating effectiveness of the data center controls.



~ SOC 1 Type 2 Compliant ~

SOC 1 Type 2 examination reports on Controls at a Service Organization in accordance with Statement on Standards for Attestation Engagements (SSAE) No. 18, reporting on controls in place for Data Center Hosting Services. Blue Hill maintains the policies and procedures and the design and operating effectiveness to comply with these regulatory requirements.

Blue Hill is PCI-DSS Compliant – Network Services

Blue Hill is enrolled in Trustwave's Trusted Commerce™ program to validate compliance with the Payment Card Industry Data Security Standard (PCI DSS) mandated by all the major credit card associations including American Express, Diners Club, Discover, JCB, MasterCard Worldwide, Visa, Inc., and Visa Europe. Blue Hill provides our PCI-DSS Attestation of Compliance and quarterly vulnerability scans to demonstrate compliance.



~ PCI-DSS Compliant for Network Services ~

Blue Hill maintains compliance with PCI requirements as set by the Payment Card Industry Security Standards by performing network security vulnerability scans for systems that store, process, or transmit cardholder data.

Blue Hill is PCI-DSS Compliant – Colocation Services

By successfully completing the annual PCI Data Security Standard (DSS) Version 3.2.1 examination, Blue Hill has demonstrated full compliance with PCI DSS requirements and security assessment procedures for the controls it has put in place at its hosted data center facility in Pearl River, NY. Blue Hill receives a Report on Compliance (ROC), which is validated with an annual on-site assessment for Attestation of Compliance (AOC) as a declaration that the results of all sections of the ROC are complete and result in an overall COMPLIANT rating.



~ PCI-DSS Compliant for Colocation Services ~

Blue Hill maintains compliance with PCI DSS requirements as set by the Payment Card Industry Security Standards and acknowledges the responsibility for the physical security of our client's hardware that store and process cardholder data, located in our data center.

Blue Hill is TRUSTe Privacy Certified

Blue Hill is responsible for its internal controls and effectiveness of its privacy programs, and the policies, disclosures, processes, and procedures described in its privacy notice.



~ TRUSTed Website Privacy Certification ~

Blue Hill's privacy policy and practices are in compliance with TRUSTe's program requirements including transparency, accountability and choice regarding the collection and use of personal information through our website.

~ TRUSTed Cloud Privacy Certification ~

Blue Hill maintains privacy and security practices for our Cloud Hosted platform clients demonstrating that data entrusted to Blue Hill by our business clients for processing, management, and storage is protected and secured, complying with the TRUSTed Cloud Privacy Certification Program Requirements.

Blue Hill is EU-U.S. and Swiss-U.S. Privacy Certified

Blue Hill receives assurance of the benefits of the Privacy Shield by annual self-certification to the U.S. Department of Commerce's International Trade Administration (ITA) that it adheres to the Privacy Shield Principles.



~ EU-U.S. and Swiss-U.S. Privacy Shield Framework ~

This Privacy Policy covers and describes how Blue Hill Data Services collects, uses, and discloses information we collect through our website and describes your choices regarding use, access, and correction of your personal information. Blue Hill participates in and has certified its compliance with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework. Blue Hill is committed to subjecting all personal data received from European Union (EU) member countries and Switzerland, respectively, in reliance on the Privacy Shield Framework, to the Framework's applicable Principles.

Blue Hill Personnel are HIPAA HITECH Privacy & Security Certified

Blue Hill employees attend and complete mandatory HIPAA and HITECH compliance training programs to maintain privacy and security practices for Protected Health Information (PHI) based on the Health Insurance Portability and Accountability Act (HIPAA) and the Health Information Technology for Economic and Clinical Health (HITECH) Act.



~ HIPAA HITECH Privacy & Security Certified ~

Blue Hill employees undergo mandatory HIPAA HITECH training in compliance with HIPAA Security and Privacy regulations to ensure the protection of data and personal health information (PHI).

Blue Hill is in Compliance with the Criminal Justice Information Services (CJIS) Security Policy through a self-attestation.

All Blue Hill solutions and services are customized per Client-specific CJIS Compliance requirements.



~ CJIS Compliance – Self Attestation ~

Blue Hill maintains vigilance over the protection and integrity of Clients' critical and confidential information through logical and physical security measures to meet and maintain compliance with regulatory and/or industry security standards. Blue Hill does not access or utilize the metadata derived from any Client for any purposes. Blue Hill will not scan any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

Blue Hill is in Compliance with the IRS Publication 1075 Tax Information Security Guidelines for Federal, State, and Local Agencies through a self-attestation.

All Blue Hill solutions and services are customized per Agency-specific IRS Publication 1075 Compliance requirements.



~ IRS Publication 1075 Compliance – Self Attestation ~

Blue Hill maintains vigilance over the protection and integrity of Agency's critical and confidential information through required logical and physical security measures to meet and maintain compliance with regulatory and/or industry security standards. Blue Hill does not access or utilize the metadata derived from any Client for any purposes. Blue Hill will not scan any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

By completing this Attestation, Blue Hill understands that we, as a consolidated data center, in conjunction with the Agency share the responsibility of protecting Federal Tax Information (FTI) data.

Blue Hill is in Compliance with International Organization for Standardization - ISO27001 Standards and Controls through our self-attestation. All Blue Hill solutions are customized to meet the specific regulatory requirements of each client.



~ ISO 27001 Standards ~

Blue Hill systematically examines information security risks, taking account threats, vulnerabilities, and impacts. We have implemented a coherent and comprehensive suite of Policies and Procedures to maintain information security controls. Blue Hill has adopted a Best-In-Class management process to ensure that the information security controls continue to meet our clients' information security requirements on an ongoing basis.

Blue Hill is in Compliance with the MARS-E volume II. Minimum Acceptable Risk Standards for Exchanges in accordance with Centers for Medicare & Medicaid Services (CMS) through a self-attestation. All Blue Hill solutions are customized to meet the specific regulatory requirements of each client.



~ MARS-E Minimum Acceptable Risk Standards for Exchanges ~

Blue Hill maintains vigilance over the protection and integrity of Clients' critical and Confidential Data, i.e., PHI, PII, and FTI through logical and physical security measures to meet and maintain compliance with regulatory and/or industry security standards as well as mandates of the Affordable Care Act of 2010. Blue Hill does not access or utilize the metadata derived from any Client for any purpose. Blue Hill will not scan any email or data files for the purpose of building analytics, data mining, advertising, or improving the services provided.

Blue Hill is GLBA and FFIEC Compliant

By successfully completing annual SOC1 Type 2 and SOC2 Type 2 examinations, Blue Hill provides the additional assurance of its security and privacy controls to our Financial Institution Clients and their clients, who run their processing environments at Blue Hill.



~ Gramm-Leach-Bliley Act ~

Blue Hill safeguards private information of individuals, the collection and disclosure of private financial information, and appropriate security for the protection of such information.



~ Federal Financial Institutions Examination Council ~

Blue Hill supports the FFIEC's uniform principles, standards, and report forms for the federal examination of financial institutions.

Blue Hill follows the data and network security requirements of each Client including multifactor authentication to protect against security breaches.



As part of Blue Hill's continuing strategy to further enhance our security standards and consistently add to our multi-layer security posture, Blue Hill is pleased to announce their strategic partnership with Cybersafe Solutions. This partnership will aid in the support of Blue Hill's corporate and customer security efforts. Cybersafe helps companies avoid expensive and disruptive cyber compromises by complementing our current defensive programs with best-in-class cyberthreat detection, live containment, and immediate response capabilities. Cybersafe supplements our multiple prevention processes by providing an additional layer of security, including 24x7 monitoring, to proactively detect any potential risks or vulnerabilities to our corporate infrastructure. This added security layer will also add to our ongoing strategy for meeting and exceeding all certification and compliance requirements.



SOC I REPORT

FOR

DATA CENTER OUTSOURCING SERVICES

**A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S
SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS**

FOR THE PERIOD MARCH 1, 2021, TO FEBRUARY 28, 2022

**PREPARED IN ACCORDANCE WITH THE
AICPA SSAE NO. 18 STANDARD**

Attestation and Compliance Services



This report is intended solely for use by the management of Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services, its user entities (i.e., customers) that utilized the services covered by this report during the specified time period, and the independent financial statement auditors of those user entities (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	4
SECTION 3	DESCRIPTION OF THE SYSTEM	7
SECTION 4	TESTING MATRICES	27

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services:

Scope

We have examined Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services' ("BHDS" or "service organization") description of its Data Center Outsourcing Services system for providing data center outsourcing services throughout the period March 1, 2021, to February 28, 2022 (the "description"), and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on criteria identified in "Management's Assertion" in Section 2 (the "assertion"). The controls and control objectives included in the description are those that management of BHDS believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Data Center Outsourcing Services system that are not likely to be relevant to user entities' internal control over financial reporting.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of BHDS's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls, as applicable, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In Section 2, BHDS has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. BHDS is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented, and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period March 1, 2021, to February 28, 2022. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;

- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- Evaluating the overall presentation of the description, suitability of the control objectives stated in the description, and suitability of the criteria specified by the service organization in its assertion.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in providing data center outsourcing services. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested, and the nature, timing, and results of those tests are listed in Section 4 (the "Testing Matrices").

Opinion

In our opinion, in all material respects, based on the criteria described in BHDS's assertion in Section 2:

- a. the description fairly presents the Data Center Outsourcing Services system that was designed and implemented throughout the period March 1, 2021, to February 28, 2022;
- b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period March 1, 2021, to February 28, 2022, and as applicable, subservice organizations and user entities applied the complementary controls assumed in the design of BHDS's controls throughout the period March 1, 2021, to February 28, 2022; and
- c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period March 1, 2021, to February 28, 2022, if, as applicable, complementary subservice organization and user entity controls assumed in the design of BHDS's controls operated effectively throughout the period March 1, 2021, to February 28, 2022.

Restricted Use

This report, including the description of the tests of controls and results thereof in the Testing Matrices, is intended solely for the information and use of management of BHDS, user entities of BHDS's Data Center Outsourcing Services system during some or all of the period March 1, 2021, to February 28, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than the specified parties.

Columbus, Ohio
April 4, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the description of Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services' ("BHDS") Data Center Outsourcing Services system for providing data center outsourcing services throughout the period March 1, 2021, to February 28, 2022 (the "description"), for user entities of the system during some or all of the period March 1, 2021, to February 28, 2022, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatement of user entities' financial statements.

The description indicates whether certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of BHDS's controls are suitably designed and operating effectively, along with related controls at BHDS. The description does not extend to controls of the user entities.

We confirm, to the best of our knowledge and belief, that:

- a. the description fairly presents the Data Center Outsourcing Services system made available to user entities of the system during some or all of the period March 1, 2021, to February 28, 2022, for providing data center outsourcing services as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:
 - i. presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, as applicable:
 - (1) the types of services provided including, as appropriate, the classes of transactions processed;
 - (2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information prepared for user entities of the system;
 - (3) the information used in the performance of the procedures including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;
 - (4) how the system captures and addresses significant events and conditions, other than transactions;
 - (5) the process used to prepare reports or other information provided for entities;
 - (6) services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them;
 - (7) the specified control objectives and controls designed to achieve those objectives, including as applicable, complementary user entity controls and complementary subservice organization controls assumed in the design of the BHDS's controls; and
 - (8) other aspects of our control environment, risk assessment process, information, and communication systems (including the related business processes), control activities, and monitoring activities that are relevant to the services provided;
 - ii. includes relevant details of changes to the Data Center Outsourcing Services system during the period covered by the description; and
 - iii. does not omit or distort information relevant to the scope of the Data Center Outsourcing Services system, while acknowledging that the description is prepared to meet the common needs of a broad

- range of user entities of the system and their user auditors, and may not, therefore, include every aspect of the Data Center Outsourcing Services system that each individual user entity of the system and its auditor may consider important in its own particular environment; and
- b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period March 1, 2021, to February 28, 2022, to achieve those control objectives if, as applicable, user entities applied complementary controls assumed in the design of BHDS's controls throughout the period March 1, 2021, to February 28, 2022. The criteria we used in making this assertion were that:
- i. the risks that threaten the achievement of the control objectives stated in the description have been identified by management of BHDS;
 - ii. the controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
 - iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Founded in 1994, Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services (BHDS) is a Tier 2 Information Technology Outsourcing (ITO) infrastructure services provider delivering fully managed, onshore data center hosting solutions and a full array of complementary IT support services to clients worldwide. BHDS specializes in Mainframe, Client Server, and AS/400 iSeries/Mid-Range managed hosting services, colocation services, dedicated high-availability disaster recovery solutions, business continuity solutions, and applications services. BHDS offers mainframe outsourcing solutions, including mainframe migration, mainframe hosting assessment, legacy applications, and software developer hosting. BHDS also provides remote server management options for clients who prefer not to relocate some or all of their servers. In this scenario, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center. The services enable clients to focus on their core business, reduce operating costs, and minimize risk while providing support on a 24 hour per day basis for their business systems. BHDS is headquartered and operates its production data center in Pearl River, New York, with two additional data centers in Branchburg, New Jersey, and Shelton, Connecticut.

Description of Services Provided

Managed Services

The managed services provided by BHDS helps ensure that client environments are proactively managed, and any issues are addressed immediately or eliminated altogether utilizing security monitoring, redundant power, communications, and environmental controls. BHDS provides support on a 24 hour per day basis for Mainframe, AS/400 iSeries/Midrange, and Client Server. Managed services support for the given platforms includes computer operations support, technical support, network support, service desk support, account management, project management, and applications maintenance and support. Services are delivered from BHDS data centers or can be delivered remotely for those clients who wish to have their equipment remain on their premises.

Mainframe Enterprise Server Management

BHDS provides custom configurations of hardware, software, networking, and services in an effort to provide an optimal outsourcing or hosting solutions. Operating environments include z/OS, OS/390, virtual machine (VM), virtual storage extended (VSE), and Linux on the mainframe. BHDS Mainframe enterprise server management support services include technical services/systems support, computer operations support, production control / job scheduling, network support, service desk, and account management.

Client Server Tools

With the ability to monitor database parameters and e-mail tasks in products such as SQL, Oracle, Exchange, Lotus Notes, etc., BHDS's Client Server monitoring helps ensure that servers are running smoothly and maximizing their availability and performance. BHDS's Client Server service integrates advanced management tools, including monitoring and alerting software, remote management capabilities, and backup and recovery software. BHDS is particularly active in virtualization of Client Server images for clients and utilizes VMware as the standard for virtualization of multiple server images onto large complex server footprints to deliver value and performance to clients. These Client Server tools automatically monitor server health, provide diagnostics, backup and restore data, and repair server issues. BHDS also hosts several UNIX server platforms (Advanced Interactive eXecutive (AIX), Solaris, Hewlett-Packard Unix (HP-UX), Linux), as well as provides remote server management options for clients who prefer not to relocate some or all of their servers. In this case, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center.

AS/400 iSeries/Midrange Management

BHDS provides hosting and support services for Midrange Servers including continuous server alert monitoring and an expert support team to help ensure issues are prevented from occurring before they impact a client's systems or their user community. BHDS also provides remote server management options for clients who prefer not to relocate some or all of their servers. In this case, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center.

Network Services

The BHDS Network Support team works with clients to design and support the local area and global data networks. BHDS enforces the client's Transmission Control Protocol (TCP)/Internet Protocol (IP) standards and helps ensure that these standards are strictly adhered to. The Network Support team provides consulting and support services to clients for various IT projects involving infrastructure, security, access, and network standards. BHDS helps ensure that bandwidth is sufficient by monitoring network data traffic. The Network Support team provides proactive analysis required to help ensure peak performance of wide area network (WAN) infrastructure, and to maintain physical network maps showing network devices in the environment. They also monitor the virtual private network (VPN) and network environment located in the data center. In addition, the Network Support team monitors clients' networks by reporting outages and key performance statistics. If an outage occurs and is circuit related, the Network Support team immediately addresses the system outage, monitors the status of the routers at each location, and notifies the given carriers. If the outage is equipment related, the client is responsible for working with their respective hardware vendors, and once the hardware is repaired, BHDS will work with the client to re-establish network connectivity.

Service Desk Services

BHDS provides robust service desk services 24x7x365 for their offerings and platforms. The service desk serves as a single point of contact by phone call or e-mail for clients and support staff. The service desk analyst proactively works to resolve requests and issues upon initial contact, and coordinates escalation and follow-up with support teams. BHDS utilizes a full featured, multi-client service desk application called information Service Desk Management System (iSDMS) to track problems, change requests, and service requests for BHDS clients. The secure cloud-based application documents related information and provides extensive search and reporting capabilities. iSDMS includes a fully customizable automated client interface that allows for the synchronization of tickets between iSDMS and the customers own service desk system. In addition, a web-based portal is available 24x7 to clients for secure self-serve access to their tickets and information.

Data Center

The production data center facility located in Pearl River, New York, covers more than 100,000 square feet including 65,000 square feet of raised floor space.

Multi-Layered Security

- Security guard station and sign-in desk for visitors at the main entrance of the building staffed on a 24 hour per day basis.
- Security guard station and sign-in desk is located outside the computer room entrance.
- Data center command station equipped with digitally recorded, continuous video surveillance cameras monitored by personnel on a 24 hour per day basis.
- Video feeds monitoring data center egress and ingress points, loading dock, colocation areas, and backup facilities.
- Multiple closed-circuit television time-lapse cameras located throughout the facility and data center.
- Badge access card system throughout the facility to control access into and throughout the facility.
- Data center visitors required to be escorted by BHDS personnel into and throughout the data center.

Redundancy

- Underground dual redundant power feeds directly from the Northeast power grid via dual diverse paths from local utility's primary transmission network.
- Diesel power generators configured with automatic transfer switches in the event of a primary power source failure.
- Uninterrupted power supply (UPS) systems in place.
- Redundant power distribution panels feed to server racks and stand-alone equipment.

- Dual redundant communications access provided by Verizon from two separate entry points into the BHDS complex.
- Tertiary diverse internet service providers (ISPs) are Internap Network Services (Internap NY PNAP, Internap NJ PNAP), Lightpath (Altice), and Crown Castle.
- Verizon Business, Verizon Core, Optimum Lightpath, and Crown Castle provide direct fiber feeds into the data center facility.
- Point-to-point Metro Ethernet connectivity directly from the data center facility to the New York Tri-State area network to provide high availability and high-capacity data transfer capabilities.
- Fully redundant ingress and egress internet access provided by Border Gateway Protocol across providers.

Environmental

- Multiple energy efficient humidification and temperature air handling systems.
- Ten 20-ton and one 12-ton Liebert computer room air-conditioning (CRAC) units in an N+1 or N+2 configuration.
- Centralized monitoring of the fire alarm system provided by building security.
- Double Interlock fire detection and suppression systems.
- Pre-action fire suppression, cross-zoned system, smoke and heat detection sensors, and hand-held fire extinguishers.
- FireSystems environmental monitoring tool to alert personnel of evacuation.
- Environmental systems monitored on a 24 hour per day basis by the central command center.
- Fault tolerant facility with a certified lightening protection system and complete building grounding system.

The Data Center Outsourcing Services system environment is responsible for providing IT services, and user entities are responsible for the procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to reports and other information presented to them; additionally, user entities are responsible for the procedures and controls governing the related accounting records, supporting information, and specific accounts that are used to initiate, authorize, record, process, and report transactions processed within the Data Center Outsourcing Services; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for those user entities.

Customers are responsible for submitting incident tickets through the iSDMS support desk ticketing system. Customer requests are recorded and track within an internal ticketing system through resolution. The ticketing system is utilized to document, prioritize, escalate, and resolve problems affecting contracted services. Customer requests are managed according to established service level agreements (SLAs).

System Boundaries

The scope of this assessment was limited to the operations performed at the Pearl River, New York, facility. The specific control objectives can be found in Section 4 of this document (the “Testing Matrices”) along with the control activities and tests of operating effectiveness.

Subservice Organizations

No subservice organizations were included in the scope of this examination.

BHDS’s Data Center Outsourcing system was designed with the assumption that no subservice organization controls were required in the design of BHDS’s controls; therefore, no control objectives related to BHDS’s Data Center Outsourcing Services system are dependent upon complementary subservice organization controls that are suitably designed and operating effectively, along with the related controls at BHDS.

Significant Changes During the Review Period

No significant changes to the Data Center Outsourcing Services system occurred during the review period.

Functional Areas of Operations

- Executive management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.
- Data center operations – responsible for managing and maintaining the command center, consoles, systems, production control/job scheduling, and service desk support for user entities on a 24 hour per day basis.
- Systems administration – responsible for specifying, deploying, and maintaining infrastructure systems, security, and technical support for user entities.
- Network engineering – responsible for specifying, deploying, and maintaining network infrastructure, security, and support for user entities.
- Facilities and building engineering – responsible for managing and protecting the physical security, environmental, electrical, and physical integrity of the building.

Infrastructure

The BHDS data center is located in Pearl River and is fully managed and supported by BHDS personnel on a 24 hour per day basis. The facility is protected by video surveillance and an electronic badge access system to control access to production infrastructure. In addition, infrastructure within the data center is supported by fully redundant power and CRAC unit configurations to allow for optimal system uptime. Network operations center (NOC) personnel monitor hardware in the data center on a real-time basis.

A series of Cisco firewalls, routers and switches, and access control lists are utilized to prevent unauthorized access to any corporate and client infrastructure.

Data Management

BHDS uses multiple tools to capture, record, and address system events. BHDS monitors its clients' systems using both real-time monitoring tools, as well as historical trend reporting tools. The iSDMS support desk ticketing system captures events related to incidents, changes, or asset management. The iSDMS support desk ticketing system is a custom-built system that interfaces with a client's specific service desk system.

BHDS utilizes the following monitoring systems:

- iSDMS – captures and reports on problem, change, and asset management events.
- I/O Concepts ioEnterprise Event Manager and Smart Client – captures mainframe system events and manages error messages.
- RevSoft Enterprise Solution Suite – utilized for monitoring and reporting of AS/400 iSeries Midrange environments.
- SolarWinds Orion and Site 24X7 – monitors open system environments and gives alerts on failed processes or connections.
- Ipswitch WhatsUp Gold IP Monitor – utilized to monitor infrastructure and network environments, alerts on failed processes or connections.
- Cisco Network Intrusion detection – monitors the corporate network.

Per the client agreed upon reporting content, BHDS delivers reports that include, but are not limited to, the following:

- Open/closed support desk tickets and outstanding/escalated incidents.
- Project status and change/asset management.
- Service level performance review.

- System performance/availability, statistics (percentage against agreed upon thresholds): Computer Processing Unit (CPU) utilization, memory capacity, channel utilization, direct access storage device (DASD) usage/storage capacity, job level performance, client information control system / time sharing option (CICS/TSO) response times, operating system availability, tape mounts/storage, and network availability.
- Upcoming disaster recovery testing, special projects, upgrades, and changes.

BHDS delivers daily, weekly, monthly, and/or quarterly reports depending on the agreed upon schedule with the client. The daily reports track status of open/closed support desk tickets. The weekly reports track open/closed service desk tickets/issues, operational issues, project status, and change management, if applicable. The monthly reports contain performance statistics along with service level reviews.

CONTROL ENVIRONMENT

The control environment at BHDS is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of BHDS's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior is the product of BHDS's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example. Specific control activities that BHDS has implemented in this area are:

- Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.
- Employees are required to sign a confidentiality agreement on an annual basis agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- New employees are required to attend a new hire orientation session as a component of the hiring process to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.
- New employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- HR personnel perform background checks for job candidates who are extended an offer of employment as a component of the hiring process.
- HR personnel require contractors to submit to a background check prior to being engaged as a contractor.
- An employee sanction procedure is in place and documented within the code of conduct communicating that an employee may be terminated for noncompliance with a policy or procedure.

Executive Management Committee Oversight

BHDS's control consciousness is influenced significantly by its executive management team. The team is comprised of experienced individuals who oversee day-to-day activities and conducts meetings to discuss matters pertinent to the organization's operational and business objectives. An executive management meeting is held on a weekly basis to discuss the performance and function of internal controls. Management holds an annual strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.

Organizational Structure and Assignment of Authority and Responsibility

BHDS's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing an organizational structure include considering key areas of authority, responsibility, and lines of reporting. BHDS's organizational structure is suited to support its strategic objectives and its customers. The appropriateness of BHDS's organizational structure depends, in part, on its size and the nature of its activities.

This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out job responsibilities. Policies and communications are directed at helping ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable. Specific control activities that BHDS has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An executive management team comprised of security personnel has been established to guide the company in managing security and availability risks.

Commitment to Competence

BHDS defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. BHDS's HR policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for hiring the most qualified individuals include emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior. Promotions driven by periodic performance appraisals demonstrate BHDS's commitment to the advancement of qualified personnel to higher levels of responsibility. In addition to position descriptions, specific controls that BHDS has implemented in this area are described below.

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- HR personnel perform screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process.
- Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.
- Hiring managers perform employee performance evaluations on an annual basis.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.
- Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.

Accountability

Management personnel establish accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. In addition to formal job descriptions and annual performance reviews, specific control activities that BHDS has implemented in this area are described below.

- Management holds an annual strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
- An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.

BHDS's HR policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities. Specific control activities that BHDS has implemented in this area are described below:

- A new hire checklist is utilized to help ensure that specific components of the hiring process are consistently executed.
- HR personnel perform screening and evaluation of job candidates in accordance with job descriptions and/or operating department management as a component of the hiring process.
- New employees are required to attend a new hire orientation session as a component of the hiring process to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.
- Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.
- Hiring managers perform employee performance evaluations on an annual basis.
- Background checks are performed for job candidates who are extended an offer of employment as a component of the hiring process.
- A termination checklist is utilized to help ensure that specific components of the termination process are consistently executed.

RISK ASSESSMENT

BHDS has implemented multiple levels of environmental redundancies to eliminate the possibility of not being able to provide services to clients, including multiple power feeds, multiple diesel power generators, multiple UPS units, multiple communications circuits, and backup disaster recovery centers in Branchburg, New Jersey and Shelton, Connecticut.

Risk Identification

BHDS assesses risk associated with the services as follows:

- Monthly executive management meetings;
- Weekly management meetings;
- Weekly change control meetings; and
- Bi-weekly operations meetings.

Areas of concentration focus on identifying the scope of risk, mitigation strategy, any vulnerabilities that may occur due to the risk, risk reduction techniques, and assigning risk assessment officers to oversee and monitor performance, legal and contractual obligations, regulatory compliance, and maintain internally developed risk mitigation processes and requirements. BHDS has specifically addressed the following areas via ongoing risk assessments:

- Staff / resource dedication / training:
 - Maintaining the highest levels of expertise, knowledge, and technology within the areas of physical and logical security, redundancy, regulatory compliance for storing, processing, and securing information.
 - Understanding current and future support requirements.
 - Skill requirements alignment with technology, including training and certification programs.
- Integrity of system data:
 - Continual assessment of data center physical security and data security, including review and update of security tools.
 - Continual assessment of network security, including review and update of security tools.
 - Continual investment and implementation of external and internal technology and security assessment tools and multi-layered security provisions.
- Technology and architecture:
 - Evaluation of hardware, software, network, and other vendors in connection with service levels (degradation), and/or recurring problems with performance and availability.
- Standard operating policies and procedures:
 - Clearly defined and documented policies and procedures and central control and coordination to help ensure standardization, consistency, and completeness to provide guidance and clear delineation of responsibilities.
 - Standard system administration procedures and acceptable use policies to allow for rapid response to any risk or change in the environment.
 - Assurance of compliance with clients' quality standards for each functional area.
 - Monitoring processes to help ensure compliance with standards.

BHDS defines severity levels, impacts, and remedies to their clients' services within the support desk escalation policies and procedures that are provided to clients, as well as in the customized SLAs for each client contract.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Risk Analysis

Risk analysis is an essential process to the entity's success. It includes identification of key business processes where potential exposures of some consequence exist. Once the significance and likelihood of risk have been assessed, management considers how the risk should be managed. This involves judgment based on assumptions about the risk, and reasonable analysis of costs associated with reducing the level of risk. Necessary actions are taken to reduce the significance or likelihood of the risk occurring, and identification of the control activities necessary to mitigate the risk. Management has identified these control activities and documented them in the Control Objectives and Related Control Activities section below. Additionally, management reviews the assessed risk levels in management meetings held on a weekly basis in which risk topics are discussed.

Integration with Control Objectives

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control objectives have been defined for each significant risk area. Control activities are then defined to serve as mechanisms for managing the achievement of those objectives and help ensure that the actions associated with those risks are carried out properly and efficiently.

CONTROL OBJECTIVES AND RELATED CONTROL ACTIVITIES

Selection and Development of Control Activities

Control activities are a part of the process by which BHDS strives to achieve its business objectives. BHDS has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, control activities are established to meet the overall objectives of the organization.

The establishment of control activities is inclusive of general control activities over technology. The management personnel of BHDS evaluate the relationships between business processes and the use of technology to perform those processes to determine the dependencies on technology. The security management processes for the technology, along with other factors, are analyzed to define and establish the necessary control activities to achieve control objectives that include technology.

The establishment of the control activities is enforced by defined policies and procedures that specifically state management's directives for BHDS personnel. The policies serve as the rules that personnel must follow when implementing certain control activities. The procedures are the series of steps the personnel should follow when performing business or technology processes and the control activities that are components of those processes.

After the policies, procedures and control activities are all established, each are implemented, monitored, reviewed, and improved when necessary.

BHDS's control objectives and related control activities are included below and also in Section 4 (the "Testing Matrices") of this report.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in the Testing Matrices, adjacent to the service organization's description of control activities. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Organization and Administration

Control Objective: Control activities provide reasonable assurance that the organization provides an adequate segregation of functions so that no person has incompatible duties that would permit the perpetration of material errors or fraud.

To help ensure that BHDS provides an adequate segregation of functions so that no person has incompatible duties that would permit the perpetration of material errors or fraud, executive management and HR personnel believe that establishing a relevant organizational structure includes considering key areas of authority and responsibility and predefined lines of reporting. An organizational chart is in place to communicate key areas of authority and responsibility and is updated as needed by executive management and HR personnel. In addition, primary service delivery units illustrated within the organizational chart, that include, but are not limited to, Mainframe services, midrange services (iSeries), network services and client server, client services, service desk, and enterprise operations are organizationally independent of each other.

Managers across each of the primary service delivery units work with HR to document written position requirements, which define the knowledge and skills necessary to accomplish tasks within each of the primary service delivery units. Furthermore, managers across key business process areas have developed documented business process policies and procedures to guide personnel in performing business processes in areas that include, but are not limited to, the following: HR, payroll, procurement, and revenue recognition. Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping ensure compliance to the policies and procedures.

Control Objective: Control activities provide reasonable assurance that an adequate segregation of functions exists between BHDS and its clients.

Documented and signed statements of work (SOWs) are in place with each client that define the services to be provided including, but not limited to, the following: nature, timing, and extent of services provided; billing schedule and rates; BHDS responsibilities; and client responsibilities. SLAs and amendments are documented by an account manager that includes the scope of changes, timeframe, and estimated costs prior to implementation. Client personnel are required to review and approve the SLA amendments prior to implementation. Account management personnel conduct meetings with client personnel on a client specified basis (e.g., weekly, bi-weekly, or monthly) to review and discuss compliance with SOW's. If any instances of non-compliance are identified during the meetings, account management personnel will document the issue within the meeting minutes and, following the meeting, investigate the cause to identify if corrective actions need to be taken. Account management personnel will then discuss the resolution with the client during the next scheduled meeting, if not before.

Clients request job scheduling changes via e-mail or verbal correspondence with a member of the service desk. Once the client submits a job scheduling request, a member of the service desk will log it into the iSDMS support desk ticketing system. The service desk representative will populate key fields within the ticket including the client name, request description, severity, and category. An operations supervisor will then identify an operator responsible for making the change via e-mail. Once the change is made, the service desk representative notifies the client via e-mail and closes the ticket.

Control Objective: Control activities provide reasonable assurance that employees involved in service delivery activities are appropriately qualified, experienced, and trained for the job functions they perform.

Prior to employment, job candidates are required to undergo screening as a job candidate in accordance with job descriptions. Following the acceptance of employment, service delivery employees and contractors are required to undergo a background check as a condition of employment. New employees are required to attend a new hire orientation session to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies. During orientation, HR personnel provide new service delivery employees with a copy of the employee manual which contains corporate policies and procedures. New hires and contractors are required to sign the confidentiality agreement acknowledgement form agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties. Additionally, employees are required to sign an acknowledgment form indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual. Upon the completion of new hire orientation, HR personnel complete a new hire checklist which documents that the new service delivery employee has been given access to the employee manual, signed the confidentiality agreement acknowledgement form, and attended new hire orientation. After a 90-day probation period, hiring managers evaluate new employees to help ensure that they can sufficiently perform the duties associated with their job function.

On an annual basis, service delivery employees are required to sign a confidentiality agreement acknowledgement form and undergo performance evaluations.

BHDS performs specific actions to remove system access and collect any company property for employees upon their departure. During the termination process, HR personnel complete a termination checklist to document that the employee returned such items as their access badge, company property (i.e., laptop), and that their system account to any BHDS systems was removed. The termination checklist is maintained within the personnel file for documentation purposes.

Physical Access Restrictions

Control Objective: Control activities provide reasonable assurance that physical access to the BHDS data center and other sensitive areas is restricted to authorized individuals.

When a new hire requires physical access to the office suite, the hiring manager completes a new employee user setup form to authorize access and submits it to the service desk via e-mail. Upon notification, the service desk opens a service desk ticket requesting that a badge access card be created for the new employee. The service desk then forwards the service desk ticket to the chief facilities engineer via e-mail. Upon notification, the chief facilities engineer activates a badge access card for issuance to the employee by HR. HR also completes a new hire checklist to document that the new employee received a badge access card.

Badge access privileges assigned to terminated employees are revoked as a component of the employee termination process. In the instance that an employee is terminated, the executive office manager or terminated employee's direct supervisor completes a termination form and submits it to the service desk via e-mail. Upon notification, the service desk opens a service desk ticket requesting that the terminated employee's badge access card be disabled. The service desk then forwards the service desk ticket to the chief facilities engineer via e-mail. Upon notification, the chief facilities engineer disables the terminated employee's badge access card. HR retrieves the terminated employee's badge access card during the employee's exit interview and completes a termination checklist in conjunction with the retrieval of the badge access card. On a monthly basis, the account manager reviews badge access privileges within the office suite and data center to help ensure that badge access privileges are authorized for each employee. In the event that unauthorized access is discovered, it is corrected, investigated, and documented within the results of the review.

Multi-Tenant Office Building

The entrance to the multi-tenant office building is staffed by third-party security personnel on a 24 hour per day basis. Visitors are required to register with the third-party security personnel during non-business hours.

Office Suite

The entrance to the office suite is locked 24 hours per day and is monitored and controlled by a receptionist during business hours. Visitors are required to sign a visitor log upon entry into the office suite. Within the visitor log, visitors document their name, date, company, and time in.

A badge access system is utilized to control access to the office suite. The badge access system utilizes pre-defined access zones so that certain areas of the office suite remain restricted. Furthermore, the badge system maintains a log of activity, allowing facilities and building engineering personnel the ability to trace access attempts to specific badges. Facilities and building engineering personnel review badge access system logs on an ad hoc basis.

Administrator access within the badge access system (i.e., the ability to add, modify, and revoke access privileges) is restricted to authorized personnel.

Data Center

Production infrastructure is located within a secure data center in locked cabinets; data center personnel maintain a list of production infrastructure that is secured within the cabinets of the data center. The ability to access the data center is restricted via the badge access system. Furthermore, the badge system maintains a log of activity that is traceable to specific badge access cards, allowing facilities and building engineering personnel the ability to trace access attempts to specific badges by reviewing the logs on an ad hoc basis.

Visitors are required to sign a visitor log upon entry into the data center. Within the visitor log, visitors document their name, date, company, and time in. While within the data center, visitors are required to be escorted by a member of facilities or operations.

Digital surveillance cameras are in place to monitor and record activity at the entrance to and throughout the data center. The digital surveillance cameras retain images/recordings for a minimum of three months.

The processes for provisioning and revoking badge access privileges for the data center follows the standard office suite processes as described above. Access to the data center is restricted to authorized personnel. Data center walls extend from the real floor to the real ceiling restricting physical access to the data center.

Property pass forms are utilized to document the removal of equipment from the data center. The chief facilities engineer, account manager, or director of strategic services is responsible for approving property pass forms.

Logical Access Restrictions

Control Objective: Control activities provide reasonable assurance that access to client system is restricted to authorized individuals.

A formal process has been established to manage user access requests, modifications, and deletions. When a new employee is hired that requires remote access to client system, an account manager submits e-mail notifications to each applicable client representative requesting access for the new employee. Technical services personnel are also copied on the e-mail notifications. Upon approval from each applicable client representative, technical services personnel provision access for the new employee based on specified requirements noted in the e-mail notifications.

Client representatives request modification of client user account access privileges via e-mail or verbal correspondence with a member of client services. Once an authorized client representative submits the request, a member of client services will log it into the iSDMS support desk ticketing system. Client services personnel log key fields within the ticket, including the client name, contact name, system, and description. Upon the creation of a ticket, client services personnel route the ticket to an operator, systems engineer, or systems administrator and the requested modifications are processed based upon the ticket. Once the requested modifications are complete, client services personnel close the ticket and notify the client representative via e-mail.

Upon notification of an employee termination from the hiring manager, technical services personnel disable the employee's VPN access to managed infrastructure. HR personnel complete a termination checklist in conjunction with the removal of access. The termination checklist is maintained within the personnel file for documentation

purposes. Terminated employees' system access rights to client systems are revoked as a component of the termination process.

In order to access the managed environment, users must first be provisioned with VPN access. VPN sessions are encrypted via transport layer security (TLS) and require two-factor authentication requiring a user account, personal identification number (PIN) code, and a Rivest-Shamir-Adleman (RSA) SecurID token. Remote access to managed environments is restricted to user accounts accessible by authorized personnel.

Upon successful authentication via the VPN system, users can authenticate to the managed infrastructure via a user account and password. The managed infrastructure is configured to enforce password requirements that include minimum length, expiration intervals, complexity requirements, minimum history, and invalid account lockout threshold.

Once in the managed infrastructure, users can access client systems. Administrator access within the managed environments is restricted to user accounts accessible by authorized personnel.

The managed infrastructure is configured to log the following events: account logon events, account management events, directory service access events, logon events, policy changes, and system events. Technical services personnel review these logs on an ad hoc basis to determine if any suspicious or unauthorized activity has occurred. In the event any suspicious or unauthorized activity occurred within the managed infrastructure, technical services personnel would investigate and follow-up for resolution.

Clients operating in a shared environment are logically segmented to help ensure confidentiality of clients' data. In addition, Open System clients run on dedicated and physically separate processing environments. Furthermore, Open System clients utilizing shared storage area network (SAN) disk storage are segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments.

Computer Operations

Control Objective: Control activities provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated to provide reasonable assurance that client institution data is processed accurately and on a timely basis.

Operations management maintains documented operations procedures to guide personnel in the execution of daily processing activities. Multiple job scheduling systems are utilized to schedule and execute daily processing activities, per client requirements. Operations personnel are available on a 24 hour per day basis to monitor processing activities for exceptions. On a daily basis, operations personnel complete a checklist to verify completion of daily processing activities to help ensure that client institution data is processed accurately and in adherence with client requirements. Multiple enterprise monitoring applications are utilized to monitor daily processing activities for exceptions and anomalies.

In the event that a job fails or if predefined thresholds are exceeded, the enterprise monitoring applications are configured to notify operations personnel via e-mail in real-time. Once notified, operations personnel review the alerts and investigate the cause. A service desk ticketing system is utilized to centrally maintain client change requests and processing routine exceptions. A member of operations will log the alert into the service desk ticketing system. Key fields within the ticket such as client name, description, severity, and category are populated. Operations personnel complete a shift log on a daily basis and document any exceptions that occurred during processing and required follow-up activities. The senior director of enterprise operations reviews daily shift logs on a weekly basis to help ensure that operations personnel are responding to any daily processing exceptions. If it is determined that daily processing exceptions are not being responded to in adherence with client requirements, the senior director of enterprise operations will investigate the cause and follow-up with the responsible member of operations for resolution.

Control Objective: Control activities provide reasonable assurance that service requests and incidents are appropriately, prioritized, logged, and tracked through resolutions and affected parties are properly notified.

Operations management maintains documented computer operations procedures to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties. The incident response procedures include defined severity levels, escalation procedures, and response time requirements for

service alerts. Incidents affecting services provided are logged in a ticketing system by operations personnel. The ticketing system provides the means to document, prioritize, track, notify, and escalate service requests and incidents that are generated by a member of operations or by a client. The incident tickets include the affected client, an initial description of the incident, and a history of the steps followed to resolve the problem. As incident tickets are logged, operations personnel utilize predefined severity levels to categorize and escalate the incident tickets. The senior director of enterprise operations reviews incident status reports on a weekly basis to monitor the status of service requests and incidents and on a frequency defined by the client, provide incident history reports to clients detailing incidents, changes, and requests logged. Operations personnel provide service desk reports to clients via e-mail on a frequency defined by the client detailing the status of logged service requests and incidents.

Control Objective: Control activities provide reasonable assurance of service availability and reliability.

Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities. Operations personnel are available on a 24 hour per day basis to monitor the operational performance of data center and client infrastructure. Operations personnel utilize multiple enterprise monitoring applications to monitor operational performance of production servers and network devices. In the event that a component of the monitored environment falls out of the pre-defined monitoring thresholds configured within the system, the enterprise monitoring applications are configured to notify operations personnel via e-mail in real-time. Once notified, operations personnel review the alerts and investigate the cause. Service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.

In order to help ensure availability and reliability for its services, redundant system architecture has been implemented so that there is no single point of failure for the production environment. Load balancing and replication devices are in place to distribute requests and provide failover services in the event of system failures. Redundant architecture includes firewalls, load balancers, servers, and internet connections. In the event that a primary load balancer or server fails, the redundant hardware is configured to take its place. Warranty and service agreements are in place for the repair and replacement of production hardware systems.

Control Objective: Control activities provide reasonable assurance that client data is backed up and safeguarded in accordance with service level agreement provisions.

Documented SLAs that define backup and recovery services for each client are in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions. Multiple backup systems are utilized to perform backups of client data according to specifications documented in the SLA. Operations personnel monitor the status of backup processing on a 24 hour per day basis. In the event of a backup failure, operations personnel create a service desk ticket and route it to technical personnel for resolution. A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media. Operations personnel rotate client backup media off-site to a third-party facility on a daily, weekly, and monthly basis in accordance with client specifications.

For clients subscribed to hot-site services, operations personnel maintain backup and recovery procedures and conduct disaster recovery tests on a frequency defined by the client.

Control Objective: Control activities provide reasonable assurance that BHDS system programs, utilities, and applications are backed up and safeguarded in an appropriate manner.

Operations personnel utilize an automated backup system to perform backups of corporate system programs, utilities, and applications. The automated backup system is configured to perform full backups of corporate system programs, utilities, and applications on a daily basis. If any backup failures occur, the backup system distributes an e-mail notification to operations personnel for investigation and resolution. Access to backup data is restricted to authorized personnel.

Control Objective: Control activities provide reasonable assurance that client service level changes are properly authorized, reviewed, approved, and implemented.

Account managers maintain documented computer operations procedures to guide employees' activities for client service specific activities including, but not limited to, client interaction, client support requests, verbal and non-verbal communications, and ticketing and escalation; additionally, procedures are in place that address the monitoring, documenting, and resolution of client support requests. Documented SLAs are in place with each client

that defines the services to be provided including, but not limited to, the following: nature, timing, and extent of services provided, billing schedule and rates, BHDS responsibilities, and client responsibilities. Client services personnel assign dedicated client services teams and supervisory personnel to each client to monitor client service activities and performance indicators and implement service level changes. Any amendments to document upgrades or modifications to existing SLAs must be approved by the client. The approvals are noted in the new amendments.

Control Objective: Control activities provide reasonable assurance that processing, maintenance, and service request activities are authorized, and changes are properly reviewed, tested, and approved prior to implementation to production.

Clients request processing, maintenance, and service requests via e-mail or verbal correspondence with a member of operations. Once a client submits a processing, maintenance, or service request, operations personnel will log it into the iSDMS service desk ticketing system. Operations personnel populate key fields within the ticket, including the client name, severity, system, category, and description. If the request is for an upgrade or release, the client services team dedicated to the client will conduct a series of meetings with the client to perform planning and preparation of the upgrade or release. Both the client and the dedicated client services team will document a timeline which includes a series of tasks that are necessary to be performed prior to implementation of the upgrade or release. Clients perform various levels of testing including user acceptance testing (UAT) and provide an approval via e-mail to the client services team prior to implementation. Operations personnel are responsible for implementing client requested processing, maintenance, and service request activities.

Control Objective: Control activities provide reasonable assurance that documentation exists that accurately and completely defines BHDS environments and is updated in a timely manner when changes are made.

Operations personnel maintain and utilize a system inventory to document system history and activity details for each client that includes the following: subsystem, utility, and program installations, as well as any upgrades, releases, and changes. As changes are made to client environments, operations personnel update the system inventory during the installation and maintenance activities to help ensure accuracy and completeness.

Telecommunications

Control Objective: Control activities provide reasonable assurance that telecommunications issues are identified and investigated in a timely manner.

Operations management maintains telecommunications procedures to guide personnel in identifying and investigating telecommunications issues. Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure. In addition, service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.

Multiple enterprise monitoring applications are utilized to monitor the health and operational performance of the production server and network devices. In the event that a component of the monitored environment falls out of the pre-defined monitoring thresholds configured within the systems, the enterprise monitoring applications are configured to notify operations personnel via e-mail in real-time. Once notified, operations personnel review the alerts and investigate the cause.

A maintenance and service agreement is in place with an ISP to provide redundancy and coverage for communications components on a 24 hour per day basis.

Control Objective: Control activities provide reasonable assurance that data transmissions between BHDS and its clients are complete, accurate, and secure.

Multiple firewall systems are in place and utilized to protect the production environment and data including filtering unauthorized inbound network traffic from the internet. External internet traffic is required to pass through the firewalls to communicate with the production servers. Any type of connection that is not explicitly authorized by the firewalls will be denied. The firewall systems are configured to log unauthorized remote access attempts to the BHDS environment and client environments. The senior director of network services and senior network engineers review firewall system logs on an ad hoc basis to identify suspicious activity and abnormal connection attempts. In the event of an invalid logon attempt, the senior director of network services and senior engineers would remove

the offending subnet from the ISP routers. Administrator access within the client and BHDS firewall systems is restricted to authorized personnel.

A third-party specialist is utilized to perform external vulnerability scans of the production network to identify potential security vulnerabilities on a monthly basis. Operations management retains the assessment report, monitors the results of the assessment within the report, and creates remediation plans to remedy any potential vulnerabilities.

Encrypted VPNs are utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network. Administrator access within the client and BHDS VPN systems is restricted to authorized personnel.

Transition

Control Objective: Control activities provide reasonable assurance that risk involved with migrating new client applications to BHDS is mitigated through formal transition planning and multiple validation testing.

Once a client has signed a SOW with BHDS for managed hosting services, account managers assign a project management team to oversee the transition process and to facilitate the resolution of any issues prior to implementation. Account managers and members of client services and support are responsible for creating the client migration plan that includes, but is not limited to, the following: timelines and due dates for the migration to BHDS, tasks and responsibilities for the client, as well as the project management team, testing requirements, and client acceptance. In addition to the creation of the client migration plan, the project management team conducts project status meetings or status updates with client personnel on a weekly basis (unless otherwise specified by the customer) via e-mail or iSDMS ticket based on client's preference. During these meetings updates, members of the project management team and client identify and review various open items that arise prior to the migration. Members of the project management team and client identify responsible parties for the completion of the open items. Once an open item has been resolved, the resolution is discussed at the next scheduled meeting update. Actions items and migration completion are documented within the e-mail thread or service desk ticket.

Prior to migration, client personnel perform multiple stages of validation testing on new client applications. Upon the successful completion of validation testing, client personnel provide a final approval illustrated via an iSDMS migration ticket or e-mail to the project management team for the migration of the application to BHDS.

INFORMATION AND COMMUNICATION SYSTEMS

Relevant Information

BHDS has integrated operational systems that allow pertinent information to be identified, captured, and communicated in sufficient detail, and, in a timeframe that allows employees to carry out their responsibilities. BHDS's information systems provide necessary information to help identify risks and opportunities, and high-quality information to manage and control activities. Information systems are developed or revised based on a strategic plan and they are relied upon for the achievement of company-level and process/application-level objectives.

Communication

Communication takes such forms as policy manuals, memorandums, and trainings. Communications also can be made electronically, verbally, and through the actions of management. When applicable, BHDS has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include orientation for new employees, training for each employee, and the use of e-mail messages to communicate time-sensitive information. Employees are encouraged to communicate to their lead/mentor, supervisor/manager, or senior/executive management.

BHDS has also implemented various methods of communication to help provide assurance that clients understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include regular meetings with representatives from different groups and service desk interactions.

If incidents are communicated, personnel follow a documented incident response plan. For example, if a change in procedure is required, the project manager is advised of the change. Formal change procedures are distributed to management before they are incorporated into the policy and distributed to relevant parties. Incidents are documented within the ticketing system and tracked by management until resolved.

MONITORING

Monitoring Activities

Management monitors controls to consider whether they are operating as intended and that the controls are modified as needed based on changes in conditions. BHDS management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policy and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two. Executive management meetings are held to review high-level severity issues and measures that were taken to alleviate the problem and to help ensure no reoccurrence of the issue. Operations personnel actively monitor production infrastructure in the data center and escalation procedures are in place to respond to exceptions in processing. Operations personnel utilize the iSDMS ticketing system to track client requests/incidents, as well as any errors that may occur in day-to-day processing routines.

Ongoing Monitoring

The BHDS management team conducts quality assurance (QA) monitoring on a regular basis and additional training is provided based upon results of monitoring procedures.

Examples of BHDS's ongoing monitoring activities include the following:

- The badge access system logs ingress and egress activity within the data center for review on an ad hoc basis.
- Surveillance cameras are in place to record activity throughout the data center.
- The data center alarm systems and building perimeter are monitored 24 hours per day.
- A building management system is configured to monitor environmental conditions within the data center and alert network operations center (NOC) personnel in the event predefined events occur.
- A ticketing system is in place to document and manage identified issues and activities impacting client services.
- Executive management meetings to review high-level severity issues and measures that were taken to alleviate the problem to help ensure no re-occurrence.
- Bi-weekly operations meetings to discuss business operations and review/improve identified problems and activities impacting client services.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing financial information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will be evaluated more often.

Often, evaluations take the form of self-assessments, where persons responsible for a particular unit or function will determine the effectiveness of controls for their activities. These assessments are considered by management, along with any other internal control evaluations. The findings of these efforts are utilized to help ensure follow-up actions are taken and subsequent evaluations are modified, as necessary.

Internal and External Auditing

BHDS supports many user entities in their efforts to meet the regulatory demands of their industry or governing agency. BHDS has assisted user entities in successfully meeting the requirements of various examination standards and regulatory demands, including:

- SOC 1 and SOC 2 examinations
- Payment Card Industry Data Security Standard (PCI DSS)

Reporting Deficiencies

Deficiencies in management’s internal control system surface from many sources, including the company’s ongoing monitoring procedures, separate evaluations of the internal control system and external parties. Management has developed protocols to help ensure findings of internal control deficiencies are reported not only to the individual responsible for the function or activity involved who is in the position to take corrective action, but also to at least one level of management above the directly responsible person. This process enables that individual to provide needed support or oversight for taking corrective action and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to deficiencies in internal control procedures and makes the decision for addressing deficiencies based on whether the incident was isolated or requires a change in the company’s procedures or personnel.

COMPLEMENTARY CONTROLS AT USER ENTITIES

BHDS’s Data Center Outsourcing Services system is designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the control objectives related to BHDS’s Data Center Outsourcing Services system to be solely achieved by BHDS’s control activities. Accordingly, user entities, in conjunction with the Data Center Outsourcing Services system, should establish their own internal controls or procedures to complement those of BHDS.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the specified control objectives described within this report are met:

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls that ensure that security procedures are established and followed to prevent the unauthorized or unintentional use of information systems and infrastructure.	Logical Access Restrictions
User entities are expected to implement controls that ensure the confidentiality of any user accounts and passwords assigned to them for use with BHDS’s systems.	
User entities are expected to implement controls that ensure that BHDS is notified of any terminations involving personnel with access to BHDS’s systems.	
User entities are expected to implement controls that ensure that username and password security practices are implemented for their applications.	
User entities are expected to implement controls that ensure that BHDS is notified of any actual or suspected information security breaches, including compromised user accounts.	

Control Activities Expected to be Implemented at User Entities	Related Control Objective
User entities are expected to implement controls that ensure that security configurations and access rights are reviewed for authorization on their applications on a periodic basis.	Logical Access Restrictions
User entities are expected to implement controls that ensure client system access requests are approved by authorized personnel.	
User entities are expected to implement controls that ensure the backups are performed of critical files, off-site backup storage, and off-site rotation of backup files for their internal systems not hosted by BHDS.	Computer Operations
User entities are expected to implement controls that define any backup, retention, and disposal requirements and for notifying BHDS of required changes.	
User entities are expected to implement controls that ensure the timely notification of any known or suspected incidents affecting services provided by BHDS.	
User entities are expected to implement controls that ensure the creation and communication of specific escalation procedures for problems to their network services and hosts.	
User entities are expected to implement controls that ensure response to known or suspected incidents reported by BHDS.	
User entities are expected to implement controls that ensure responsibility for monitoring the adherence to and requesting changes to SLAs maintained within BHDS.	
User entities are expected to implement controls that ensure BHDS is notified of required changes to their solutions in a timely manner.	
User entities are expected to implement controls that ensure performance of additions, changes, or deletions to the list of authorized personnel in a timely manner.	
User entities are expected to implement controls that ensure that defined communication methods are utilized to connect to BHDS' systems (e.g., direct connections, over public networks, etc.)	Telecommunications
User entities are expected to implement controls that ensure the review, testing, and approval of software integrations for completeness and accuracy.	Transition

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Data Center Outsourcing Services system provided by BHDS. The scope of the testing included the applicable controls for the Data Center Outsourcing Services system considered to be relevant to the internal control over financial reporting of respective user entities. Schellman & Company, LLC (Schellman) conducted the examination testing over the period March 1, 2021, to February 28, 2022.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the specified control objectives were achieved during the period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during testing. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant evidentiary matter records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible and evaluated for accuracy and completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than the aforementioned constitutes a test result that is the result of a change in the application of the control activity, a deficiency in the operating effectiveness of the control activity, or a disclosure related to the non-occurrence of the condition(s) that would warrant the operation of the control. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls at user entities, as this determination can only be made after consideration of controls in place at user entities, and other factors. Control considerations that should be implemented by user entities in order to complement the control activities and achieve the stated control objective are presented in the “Complementary Controls at User Entities” within Section 3.

ORGANIZATION AND ADMINISTRATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that the organization provides an adequate segregation of functions so that no person has incompatible duties that would permit the perpetration of material errors or fraud.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.01	Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.	Inquired of the director of office administration regarding organizational charts to determine that organizational charts were in place to communicate key areas of authority and responsibility and that the charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organizational chart to determine that organizational charts were in place and identified key areas of authority and responsibility.	No exceptions noted.
1.02	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.03	Primary service delivery units and teams are organizationally independent of each other.	Inspected the organizational chart to determine that primary service delivery units and teams were organizationally independent of each other.	No exceptions noted.
1.04	<p>Documented business process procedures are in place to guide personnel in key business processes including, but not limited to, the following:</p> <ul style="list-style-type: none"> • HR • Payroll • Procurement • Revenue recognition and deferred accounting 	<p>Inspected the business process procedures to determine that documented business process procedures were in place to guide personnel in key business processes that included the following:</p> <ul style="list-style-type: none"> • HR • Payroll • Procurement • Revenue recognition and deferred accounting 	No exceptions noted.
1.05	Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.	Inquired of the director of office administration regarding manager practices to determine that managers were actively involved in supervising and reviewing the work of subordinate employees and were responsible for helping to ensure compliance to client and company operating procedures.	No exceptions noted.
		Inspected the business process procedures to determine that managers were actively involved in supervising and reviewing the work of subordinate employees.	No exceptions noted.

[Intentionally Blank]

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that an adequate segregation of functions exists between BHDS and its clients.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.01	<p>A signed SOW is maintained with clients that define the services to be provided that includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> • Nature, timing, and extent of services provided • Billing schedule and rates • BHDS responsibilities • Client responsibilities 	<p>Inspected the signed SOWs for a sample of current clients to determine that a signed SOW was maintained for each client sampled that included the following:</p> <ul style="list-style-type: none"> • Nature, timing, and extent of services provided • Billing schedule and rates • BHDS responsibilities • Client responsibilities 	No exceptions noted.
2.02	An account manager completes an SLA amendment for client service level changes that includes the scope of changes, timeframe, and estimated costs prior to implementation.	Inquired of the director of strategic services regarding client service level changes to determine that an account manager completed an SLA amendment for client service level changes prior to implementation.	No exceptions noted.
		Inspected the SLA amendments for a sample of SLA changes during the review period to determine that a service level amendment documenting the scope of changes, timeframe, and estimated costs was completed for each change sampled.	No exceptions noted.
2.03	Account management personnel require client personnel to review and approve SLA amendments prior to implementation.	Inquired of the director of strategic services regarding client service level changes to determine that account management personnel required client personnel to review and approve SLA amendments prior to implementation.	No exceptions noted.
		Inspected evidence of approval for a sample of SLA changes during the review period to determine that client personnel reviewed and approved SLA amendments for each change sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.04	A service desk ticketing system is utilized to centrally maintain client change requests and processing routine exceptions.	Inspected the service desk tickets for a sample of client changes and processing exceptions generated during the review period to determine that a service desk ticketing system was utilized to centrally maintain client change requests and processing routine exceptions for each client change and processing exception sampled.	No exceptions noted.
2.05	Account management personnel conduct meetings with client personnel on a client specified basis to review and discuss compliance with SOWs.	Inquired of the director of strategic services regarding SOW compliance to determine that account management personnel conducted meetings with client personnel on a client specified basis to review and discuss compliance with SOWs.	No exceptions noted.
		Inspected the recurring meeting invite for a sample of current clients to determine that meetings were conducted on a client specified basis during the review period for each client sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that employees involved in service delivery activities are appropriately qualified, experienced, and trained for the job functions they perform.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
New Employees and Contractors			
3.01	A new hire checklist is utilized to help ensure that specific components of the hiring process are consistently executed.	Inspected the new hire checklist for a sample of employees hired during the review period to determine that a new hire checklist was utilized to help ensure that specific components of the hiring process were consistently executed for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.02	HR personnel perform screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process.	Inquired of the director of office administration regarding the hiring process to determine that HR personnel performed screening and evaluation of job candidates in accordance with job descriptions.	No exceptions noted.
		Inspected evidence of screening and evaluation for a sample of employees hired during the review period to determine that HR personnel performed screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process for each employee sampled.	No exceptions noted.
3.03	HR personnel perform background checks for job candidates who are extended an offer of employment as a component of the hiring process.	Inspected evidence of background check performance for a sample of employees hired during the review period to determine that HR personnel performed background checks for job candidates who were extended an offer of employment as a component of the hiring process for each employee sampled.	No exceptions noted.
3.04	New employees are required to attend a new hire orientation session as a component of the hiring process to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.	Inquired of the director of office administration regarding the hiring process to determine that new employees were required to attend a new hire orientation session as a component of the hiring process to help ensure that they were familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.	No exceptions noted.
		Inspected evidence of new hire orientation session attendance for a sample of employees hired during the review period to determine that new employees attended a new hire orientation session as a component of the hiring process for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.05	New employees and contractors are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreements for a sample of employees and contractors hired during the review period to determine that new employees and contractors were required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties for each employee and contractor sampled.	No exceptions noted.
3.06	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.	Inspected the acknowledgement forms for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual for each employee sampled.	No exceptions noted.
3.07	Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.	Inquired of the director of office administration regarding the hiring process to determine that hiring managers evaluated new employees after a 90-day probation period to help ensure that they were able to sufficiently perform the duties associated with their job function.	No exceptions noted.
		Inspected the 90-day evaluations for a sample of employees hired during the review period to determine that a hiring manager completed an evaluation after the 90-day probation period for each employee sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.08	HR personnel require contractors to submit to a background check as a component of the contract engagement process.	Inspected evidence of background check completion for a sample of contractors hired during the review period to determine that HR personnel performed required contractors to submit to a background check as a component of the engagement process for each contractor sampled.	No exceptions noted.
Current Employees			
3.09	Employees are required to sign a confidentiality agreement on an annual basis agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreements for a sample of current employees to determine that employees were required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties during the review period for each employee sampled.	No exceptions noted.
3.10	Hiring managers perform employee performance evaluations on an annual basis.	Inspected the employee performance evaluations for a sample of current employees to determine that hiring managers performed employee performance evaluations during the review period for each employee sampled.	No exceptions noted.
Terminated Employees			
3.11	A termination checklist is utilized to help ensure that specific components of the termination process are consistently executed.	Inspected the termination checklist for a sample of employees terminated during the review period to determine that a termination checklist was utilized to help ensure that specific components of the termination process were consistently executed for each terminated employee sampled.	No exceptions noted.

PHYSICAL ACCESS RESTRICTIONS

Control Objective Specified Control activities provide reasonable assurance that physical access to the BHDS by the Service Organization: data center and other sensitive areas is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.01	Hiring managers provide authorization prior to physical access privileges being granted to new employees.	Inquired of the director of office administration regarding physical access restrictions to determine that hiring managers provided authorization prior to physical access privileges being granted to new employees.	No exceptions noted.
		Inspected evidence of authorization for a sample of employees hired during the review period to determine that hiring managers provided authorization to grant physical access privileges for each employee sampled.	No exceptions noted.
4.02	Badge access privileges assigned to terminated employees are revoked as a component of the employee termination process.	Inquired of the chief facilities engineer regarding the termination process to determine that badge access privileges assigned to terminated employees were revoked as a component of the employee termination process.	No exceptions noted.
		Inspected the badge access listing for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
4.03	An account manager reviews badge access privileges on a monthly basis to help ensure that badge access privileges are authorized.	Inquired of an account manager regarding the review of badge access privileges to determine that an account manager reviewed badge access privileges on a monthly basis to help ensure that badge access privileges were authorized.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the badge access privileges review documentation for a sample of months during the review period to determine that an account manager reviewed badge access privileges for each month sampled.	No exceptions noted.
Multi-Tenant Office Building			
4.04	The entrance to the multi-tenant office building is staffed by third-party security personnel 24 hours per day.	Inquired of the director of strategic services regarding building security to determine that the entrance to the multi-tenant building was staffed by third-party security personnel 24 hours per day.	No exceptions noted.
		Observed the third-party security personnel to determine that the entrance to the multi-tenant office building was staffed by third-party security personnel.	No exceptions noted.
4.05	Visitors are required to register with third-party security personnel during non-business hours.	Inquired of the chief facilities engineer regarding visitor registration to determine that visitors were required to register with third-party security personnel during non-business hours.	No exceptions noted.
		Inspected an example visitor log during the review period to determine that visitors were required to register with third-party security personnel during non-business hours.	No exceptions noted.
Office Suite			
4.06	The entrance to the office suite is locked 24 hours per day and is monitored and controlled by a receptionist during business hours.	Inquired of the director of strategic services regarding the office suite to determine that the entrance to the office suite was locked 24 hours per day and was monitored and controlled by a receptionist during business hours.	No exceptions noted.
		Observed the entrance to the office suite to determine that the entrance to the office suite was monitored and controlled by a receptionist during business hours.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.07	Visitors are required to sign a visitor log upon entering the office suite.	Observed the visitor entrance process to determine that visitors were required to sign a visitor log upon entering the office suite.	No exceptions noted.
		Inspected the office suite visitor logs for a sample of months during the review period to determine that visitor logs were in place for each month sampled.	No exceptions noted.
4.08	A badge access system is utilized to control access to the office suite.	Observed the badge access system throughout the office suite to determine that a badge access system was utilized to control access to the office suite.	No exceptions noted.
		Inspected the badge access listing and zone definitions to determine that a badge access system was utilized to control access to the office suite.	No exceptions noted.
4.09	Administrator access within the badge access system is restricted to user accounts accessible by authorized personnel.	Inspected the badge access system administrator account listing with the assistance of the chief facilities engineer to determine that administrator access within the badge access system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
4.10	The badge access system logs access attempts that are traceable to specific badge access cards. Facilities and building engineering personnel review badge access system logs on an ad-hoc basis.	Inquired of the chief facilities engineer regarding the badge access system to determine that facilities and building engineering personnel reviewed badge access system logs on an ad-hoc basis.	No exceptions noted.
		Inspected an example badge access system log generated during the review period to determine that the badge access system logged access attempts that were traceable to specific badge access cards.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Data Center		
4.11	Production infrastructure is housed within a secure data center.	Observed the production infrastructure located within the data center to determine that production infrastructure was housed within a secure data center.	No exceptions noted.
4.12	Data center personnel maintain a list of production infrastructure that is secured within the data center.	Inspected the production infrastructure listing to determine that data center personnel maintained a list of production infrastructure that was secured within the data center.	No exceptions noted.
4.13	Production infrastructure is secured in locked cabinets within the data center.	Observed the production infrastructure to determine that production infrastructure was secured in locked cabinets within the data center.	No exceptions noted.
4.14	Property pass forms are utilized to document the removal of equipment from the data center. Property pass forms are required to be approved by personnel holding one of the following positions: <ul style="list-style-type: none"> • Chief facilities engineer • Account manager • Director strategic services 	Inquired of the chief facilities engineer regarding property pass forms to determine that property pass forms were utilized to document the removal of equipment from the data center and that property pass forms were required to be approved by personnel holding one of the following positions: <ul style="list-style-type: none"> • Chief facilities engineer • Account manager • Director strategic services 	No exceptions noted.
		Inspected evidence of approval for a sample of property pass forms documented during the review period to determine that each equipment removal sampled was approved by personnel holding one of the following positions: <ul style="list-style-type: none"> • Chief facilities engineer • Account manager • Director strategic services 	No exceptions noted.
4.15	A badge access system is utilized to control access to the data center.	Observed the badge access system to determine that a badge access system was utilized to control access to the data center.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the badge access listing and zone definitions to determine that a badge access system was utilized to control access to the data center.	No exceptions noted.
4.16	The badge access system logs access attempts that are traceable to specific badge access cards. Facilities and building engineering personnel review badge access system logs on an ad-hoc basis.	Inquired of the chief facilities engineer regarding the badge access system to determine that facilities and building engineering personnel reviewed badge access system logs on an ad-hoc basis.	No exceptions noted.
		Inspected an example badge access system log generated during the review period to determine that the badge access system logged access attempts that were traceable to specific badge access cards.	No exceptions noted.
4.17	Administrator access within the badge access system is restricted to user accounts accessible by authorized personnel.	Inspected the badge access system administrator account listing with the assistance of the chief facilities engineer to determine that administrator access within the badge access system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
4.18	Visitors are required to be escorted when accessing the data center.	Observed the visitor access process to determine that visitors were required to be escorted when accessing the data center.	No exceptions noted.
4.19	Visitors are required to sign a visitor log upon entering the data center.	Observed the visitor entrance process to determine that visitors were required to sign a visitor log upon entering the data center.	No exceptions noted.
		Inspected the data center visitor logs for a sample of months during the review period to determine that visitor logs were in place for each month sampled.	No exceptions noted.
4.20	A digital surveillance system is in place to monitor and record activity at the entrance to and throughout the data center.	Observed the digital surveillance cameras throughout the data center to determine that a digital surveillance system was in place to monitor and record activity at the entrance to and throughout the data center.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected an example historical image recorded during the review period to determine that a digital surveillance system was in place to monitor the data center.	No exceptions noted.
4.21	Recordings from the digital surveillance cameras are retained for a minimum of three months.	Inspected an example historical image recorded during the review period to determine that recordings from the digital surveillance cameras were retained for a minimum of three months.	No exceptions noted.
4.22	Access to the data center is restricted to badge access cards assigned to authorized personnel.	Inspected the data center access listing with the assistance of the director of strategic services to determine that access to the data center was restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
4.23	Data center walls extend from the real floor to the real ceiling restricting physical access to the data center.	Observed the data center walls to determine that data center walls extended from the real floor to the real ceiling restricting physical access to the data center.	No exceptions noted.

LOGICAL ACCESS RESTRICTIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that access to client system is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.01	Operations personnel require authorization from an authorized client representative for the modification of client user account access privileges.	Inquired of the director of strategic services regarding authorization for the modification of client user account access privileges to determine that operations personnel required authorization from an authorized client representative for the modification of client user account access privileges.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of authorization for a sample of client user account access privilege modification requests during the review period to determine that authorization from a client representative was obtained for each request sampled.	No exceptions noted.
5.02	Terminated employees' system access rights to client systems are revoked as a component of the termination process.	Inspected the client system user access privileges for a sample of client systems and employees terminated during the review period to determine that access privileges to client systems were revoked for each client system and terminated employee sampled as a component of the termination process.	No exceptions noted.
Managed Infrastructure Authentication			
5.03	Access to managed infrastructure is secured via an encrypted VPN that requires two-factor authentication using RSA SecurID technology that includes the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	Observed the VPN authentication process to determine that access to managed infrastructure required two-factor authentication using RSA SecurID technology that included the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	No exceptions noted.
		Inspected the VPN and RSA system configurations to determine that access to managed infrastructure was secured via an encrypted VPN that required two-factor authentication using RSA SecurID technology.	No exceptions noted.
5.04	The VPN system is configured to encrypt communication sessions between the managed environment and user entities via TLS.	Inspected the VPN system configurations to determine that the VPN was configured to encrypt communication sessions between the managed environment and user entities via TLS.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.05	<p>The managed infrastructure is configured to enforce the following user account and password controls:</p> <ul style="list-style-type: none"> • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history • Invalid password account lockout threshold 	<p>Inspected the managed infrastructure authentication configurations to determine that the managed infrastructure was configured to enforce the following user account and password controls:</p> <ul style="list-style-type: none"> • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history • Invalid password account lockout threshold 	No exceptions noted.
Managed Infrastructure Access			
5.06	Administrator access within the managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the user access permissions for a sample of client systems with the assistance of the director of strategic services to determine that administrator access within the managed environment was restricted to user accounts accessible by authorized personnel for each client system sampled.	No exceptions noted.
5.07	Remote access to managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with remote access to managed environments with the assistance of the director of strategic services to determine that remote access to managed environments was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
5.08	Shared processing environments are logically segmented to help ensure the confidentiality of client data.	Inspected evidence of logical segmentation for a sample of current clients operating in a shared processing environment to determine that shared processing environments were logically segmented to help ensure the confidentiality of client data for each client sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.09	Open system environments run on dedicated and physically separate processing environments.	Inspected the physical system inventories for a sample of open system clients to determine that open system environments ran on dedicated and physically separate processing environments for each client sampled.	No exceptions noted.
5.10	Open system environments utilizing shared SAN disk storage are segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments.	Inspected the SAN disk configurations for a sample of open system clients utilizing shared SAN disk storage to determine that open system environments utilizing SAN disk storage were segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments for each client sampled.	No exceptions noted.
Managed Infrastructure Monitoring and Logging			
5.11	<p>The managed infrastructure is configured to log the following events:</p> <ul style="list-style-type: none"> • Account logon events • Account management events • Directory service access events • Logon events • Policy changes • System events <p>Technical services personnel review managed infrastructure logs on an ad hoc basis.</p>	Inquired of the director of strategic services regarding the managed infrastructure log review process to determine that technical services personnel reviewed managed infrastructure logs on an ad hoc basis.	No exceptions noted.
		<p>Inspected the managed infrastructure logging configurations and an example event log generated during the review period to determine that the managed infrastructure was configured to log the following events:</p> <ul style="list-style-type: none"> • Account logon events • Account management events • Directory service access events • Logon events • Policy changes • System events 	No exceptions noted.

COMPUTER OPERATIONS

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that authorized programs are executed as planned and deviations from scheduled processing are identified and investigated to provide reasonable assurance that client institution data is processed accurately and on a timely basis.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.01	Documented computer operations procedures are in place to guide personnel in the execution of daily processing activities.	Inspected the computer operations procedures for a sample of current clients to determine that documented computer operations procedures were in place to guide personnel in the execution of daily processing activities for each client sampled.	No exceptions noted.
6.02	Multiple job scheduling systems are utilized to schedule and execute daily processing activities per client requirements.	Inspected the turnover reports for a sample of current clients and dates during the review period to determine that a job scheduling system was utilized to schedule and execute daily processing activities for each client and date sampled.	No exceptions noted.
6.03	Operations personnel complete a checklist on a daily basis to help ensure that client institution data is processed accurately and in adherence with client requirements.	Inspected the operations checklists for a sample of dates during the review period to determine that operations personnel completed a checklist to help ensure that client institution data was processed accurately and in adherence with client requirements for each date sampled.	No exceptions noted.
6.04	Operations personnel are available on a 24 hour per day basis to monitor processing activities for exceptions.	Inquired of the director of strategic services regarding processing activities monitoring to determine that operations personnel were available on a 24 hour per day basis to monitor processing activities for exceptions.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available on a 24 hour per day basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.05	Enterprise monitoring applications are utilized to monitor processing activities for exceptions and anomalies.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor processing activities for exceptions and anomalies.	No exceptions noted.
6.06	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded, or controlled events are triggered.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded, or controlled events were triggered.	No exceptions noted.
6.07	A service desk ticketing system is utilized to centrally maintain client change requests and processing routine exceptions.	Inspected the service desk tickets for a sample of client changes and processing exceptions generated during the review period to determine that a service desk ticketing system was utilized to centrally maintain client change requests and processing routine exceptions for each client change and processing exception sampled.	No exceptions noted.
6.08	Operations personnel complete a shift log on a daily basis and document any exceptions that occurred during processing and required follow-up activities.	Inspected the shift logs for a sample of dates during the review period to determine that operations personnel completed a shift log and documented any exceptions that occurred during processing and required follow-up activities for each date sampled.	No exceptions noted.
6.09	The supervisor of enterprise operations reviews shifts logs on a weekly basis to help ensure response to processing exceptions occurs.	Inspected evidence of shift log reviews for a sample of weeks during the review period to determine that the supervisor of enterprise operations reviewed shifts logs to help ensure response to processing exceptions occurred for each week sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that service requests and incidents are appropriately, prioritized, logged, and tracked through resolutions and affected parties are properly notified.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.01	Documented computer operations procedures are in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	Inspected the computer operations procedures to determine that documented computer operations procedures were in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	No exceptions noted.
7.02	An automated ticketing system is utilized to prioritize, log, and track resolution steps for service requests and incidents.	Inspected the incident tickets for a sample of service requests and incidents logged during the review period to determine that an automated ticketing system was utilized to prioritize, log, and track resolution steps for service requests and incidents for each service request and incident sampled.	No exceptions noted.
7.03	Operations personnel utilize predefined severity levels to prioritize and escalate service requests and incidents.	Inspected the incident ticket severity levels for a sample of service requests and incidents logged during the review period to determine that operations personnel utilized predefined severity levels to prioritize and escalate service requests and incidents for each service request and incident sampled.	No exceptions noted.
7.04	The supervisor of enterprise operations reviews incident status reports on a weekly basis to monitor the status of service requests and incidents.	Inquired of the director of strategic services regarding the review of incident status reports to determine that the supervisor of enterprise operations reviewed incident status reports on a weekly basis to monitor the status of service requests and incidents.	No exceptions noted.
		Inspected the incident status report review for a sample of weeks during the review period to determine that the supervisor of enterprise operations reviewed incident status reports for each week sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.05	Operations personnel provide service desk reports to clients via e-mail on a frequency defined by the client detailing the status of logged service requests and incidents.	Inspected the service desk reports for a sample of current clients and dates, weeks, and months during the review period to determine that operations personnel provided service desk reports via e-mail on a frequency defined by the client detailing the status of logged service requests and incidents for each client and date, week, and month sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance of service availability and reliability.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.01	Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities.	Inspected the incident response procedures to determine that documented incident response procedures were in place to guide personnel in server and network outage response, escalation, and resolution activities.	No exceptions noted.
8.02	Enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor operational performance of production servers and network devices.	No exceptions noted.
8.03	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
8.04	Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure.	Inquired of the director of strategic services regarding data center and client infrastructure monitoring to determine that operations personnel were available on a 24 hour per day basis to monitor data center and client infrastructure.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available on a 24 hour per day basis.	No exceptions noted.
8.05	Service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.	Inspected the staffing schedule for a sample of months during the review period to determine that service desk personnel were available on a 24 hour per day basis to monitor client environments and respond to support requests for each month sampled.	No exceptions noted.
8.06	Warranty and service agreements are in place for the repair and replacement of production hardware systems.	Inspected the warranty and service agreements to determine that warranty and service agreements were in place for the repair and replacement of production hardware systems.	No exceptions noted.
8.07	Load balancing and replication devices are in place to distribute requests and provide failover services in the event of system failures.	Inspected the load balancing and replication device configurations to determine that load balancing and replication devices were in place to distribute requests and provide failover services in the event of system failures.	No exceptions noted.

Control Objective Specified Control activities provide reasonable assurance that client data is backed up and
by the Service Organization: safeguarded in accordance with service level agreement provisions.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.01	Documented SLAs that define backup and recovery services for clients are in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions.	Inspected the SLAs for a sample of current clients subscribed to disaster recovery services to determine that documented SLAs that defined backup and recovery services were in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions for each client sampled.	No exceptions noted.
9.02	Multiple backup systems are utilized to perform backups of client data according to specifications documented in the SLA.	Inspected the backup system configurations and example backup logs generated during the review period for a sample of current clients subscribed to data backup services to determine that multiple backup systems were utilized to perform backups of client data according to specifications documented in the SLA for each client sampled.	No exceptions noted.
9.03	Operations personnel monitor the status of backup processing on a 24 hour per day basis. Processing errors are reported to technical personnel for resolution and documented in a service desk ticket.	Inquired of the director of strategic services regarding backup monitoring to determine that operations personnel monitored the status of backup processing on a 24 hour per day basis.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available to monitor the status of backup processing on a 24 hour per day basis.	No exceptions noted.
		Inspected the service desk tickets for a sample of processing errors generated during the review period to determine that processing errors were reported to technical personnel for resolution and documented in a service desk ticket for each processing error sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
9.04	A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	Inspected the third-party media storage agreement to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	No exceptions noted.
		Inspected the third-party media storage invoices for a sample of months during the review period to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media for each month sampled.	No exceptions noted.
9.05	Operations personnel rotate backup media to the off-site third-party media vaulting company on a daily, weekly, and monthly basis in accordance with client specifications.	Inspected the tape transfer manifests for a sample of current clients subscribed to managed backup and tape rotation services and dates, weeks, and months during the review period to determine that operations personnel rotated backup media to the off-site third-party media vaulting company in accordance with client specifications for each client, date, week, and month sampled.	No exceptions noted.
9.06	Operations personnel maintain backup and recovery procedures for clients subscribed to hot-site services and are tested according to client requirements.	Inspected the backup and recovery procedures for a sample of current clients subscribed to hot-site services to determine that operations personnel maintained backup and recovery procedures for each client sampled.	No exceptions noted.
		Inspected the most recent backup and recovery test results for a sample of current clients subscribed to hot-site services to determine that backup and recovery procedures were tested during the review period for each client sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that BHDS system programs, utilities, and applications are backed up and safeguarded in an appropriate manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
10.01	An automated backup system is utilized to perform backups of corporate system programs, utilities, and applications.	Inspected the backup system configurations and an example backup log generated during the review period to determine that an automated backup system was utilized to perform backups of corporate system programs, utilities, and applications.	No exceptions noted.
10.02	The automated backup system is configured to perform full backups of corporate system programs, utilities, and applications on a daily basis.	Inspected the backup system configurations and backup logs generated during the review period to determine that the automated backup system was configured to perform full backups of corporate system, programs, utilities, and applications on a daily basis.	No exceptions noted.
10.03	The automated backup system is configured to send e-mail alert notifications to operations personnel regarding backup job completion status.	Inspected the backup alert notification configurations and an example e-mail alert notification generated during the review period to determine that the automated backup system was configured to send e-mail alert notifications to operations personnel regarding backup job completion status.	No exceptions noted.
10.04	Access to backup data is restricted to user accounts accessible by authorized personnel.	Inspected the system-generated listing of user accounts with access to backup data with the assistance of the director of strategic services to determine that access to backup data was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that client service level changes are properly authorized, reviewed, approved, and implemented.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
11.01	Documented computer operations procedures are in place to guide personnel in client service specific activities that include, but are not limited to, the following: <ul style="list-style-type: none"> • Client interaction • Verbal and non-verbal communications • Ticketing and escalation 	Inspected the computer operations procedures to determine that documented computer operations procedures were in place to guide personnel in client service specific activities that included the following: <ul style="list-style-type: none"> • Client interaction • Verbal and non-verbal communications • Ticketing and escalation 	No exceptions noted.
11.02	Documented computer operations procedures are in place that address the monitoring, documenting, and resolution of client support requests.	Inspected the computer operations procedures to determine that documented computer operations procedures were in place that addressed the monitoring, documenting, and resolution of client support requests.	No exceptions noted.
11.03	Dedicated client services teams and supervisory personnel are assigned to monitor client service activities and performance indicators and implement service level changes.	Inquired of the director of strategic services regarding client service teams to determine that dedicated client service teams and supervisory personnel were assigned to monitor client service activities and performance indicators and implement service level changes.	No exceptions noted.
		Inspected the client services teams and supervisory personnel assignments for a sample of current clients to determine that client services teams and supervisory personnel were assigned to each client sampled.	No exceptions noted.
11.04	An account manager completes an SLA amendment for client service level changes that includes the scope of changes, timeframe, and estimated costs prior to implementation.	Inquired of the director of strategic services regarding client service level changes to determine that an account manager completed an SLA amendment for client service level changes prior to implementation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the SLA amendments for a sample of SLA changes during the review period to determine that a service level amendment documenting the scope of changes, timeframe, and estimated costs was completed for each change sampled.	No exceptions noted.
11.05	Account management personnel require client personnel to review and approve SLA amendments prior to implementation.	Inquired of the director of strategic services regarding client service level changes to determine that account management personnel required client personnel to review and approve SLA amendments prior to implementation.	No exceptions noted.
		Inspected evidence of approval for a sample of SLA changes during the review period to determine that client personnel reviewed and approved SLA amendments for each change sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that processing, maintenance, and service request activities are authorized, and changes are properly reviewed, tested, and approved prior to implementation to production.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
12.01	An automated ticketing system is utilized to prioritize, log, and track resolution steps for processing, maintenance, and service request activities.	Inspected the service desk tickets for a sample of processing, maintenance, and service request activities logged during the review period to determine that an automated ticketing system was utilized to prioritize, log, and track resolution steps for each activity sampled.	No exceptions noted.
12.02	Operations management requires client personnel to perform UAT for upgrades prior to implementation.	Inquired of the director of strategic services regarding upgrades to determine that operations management required client personnel to perform UAT for upgrades prior to implementation.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of UAT for a sample of upgrades implemented during the review period to determine that client personnel performed UAT for each upgrade sampled.	No exceptions noted.
12.03	Operations management requires client personnel to approve upgrades prior to implementation.	Inquired of the director of strategic services regarding upgrades to determine that operations management required client personnel to approve upgrades prior to implementation.	No exceptions noted.
		Inspected evidence of approval for a sample of upgrades implemented during the review period to determine that client personnel approved each upgrade sampled.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that documentation exists that accurately and completely defines BHDS environments and is updated in a timely manner when changes are made.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
13.01	Operations personnel maintain and utilize a system inventory and ticketing system to document system history and activity details including, but not limited to, the following: <ul style="list-style-type: none"> • Subsystem, utility, and program installations • Upgrades, releases, and changes 	Inspected the system inventories and system maintenance tickets for sample of current clients to determine that a system inventory and ticketing system was maintained and utilized to document system history and activity details for each client sampled that included the following: <ul style="list-style-type: none"> • Subsystem, utility, and program installations • Upgrades, releases, and changes 	No exceptions noted.
13.02	Operations personnel update the system inventory during installation and maintenance activities.	Inspected the system inventory and system maintenance tickets for a sample of current clients to determine that operations personnel updated the system inventory during installation and maintenance activities for each client sampled.	No exceptions noted.

TELECOMMUNICATION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that telecommunications issues are identified and investigated in a timely manner.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.01	Documented telecommunications procedures are in place to guide personnel in identifying and investigating telecommunications issues.	Inspected the telecommunications procedures to determine that documented telecommunications procedures were in place to guide personnel in identifying and investigating telecommunications issues.	No exceptions noted.
14.02	Enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor operational performance of production servers and network devices.	No exceptions noted
14.03	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
14.04	Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure.	Inquired of the director of strategic services regarding data center and client infrastructure monitoring to determine that operations personnel were available on a 24 hour per day basis to monitor data center and client infrastructure.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available on a 24 hour per day basis.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
14.05	Service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.	Inspected the staffing schedule for a sample of months during the review period to determine that service desk personnel were available on a 24 hour per day basis to monitor client environments and respond to support requests for each month sampled.	No exceptions noted.
14.06	A maintenance and service agreement is in place with an ISP to provide coverage for communications components on a 24 hour per day basis.	Inquired of the director of strategic services regarding the ISP to determine that a maintenance and service agreement was in place with an ISP to provide coverage for communications components on a 24 hour per day basis.	No exceptions noted.
		Inspected the maintenance and service agreement for the ISP to determine that a maintenance and service agreement was in place with an ISP to provide coverage for communications components.	No exceptions noted.

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that data transmissions between BHDS and its clients are complete, accurate, and secure.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Firewall Systems		
15.01	Firewall systems are in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall system configurations for a sample of firewall systems to determine that firewall systems were in place to filter unauthorized inbound network traffic from the internet for each firewall sampled.	No exceptions noted.
15.02	The firewall systems are configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall system configurations for a sample of firewall systems to determine that the firewall systems were configured to deny any type of network connection that was not explicitly authorized by a firewall rule for each firewall sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
15.03	The firewall systems are configured to log unauthorized remote access attempts to the BHDS environment and client environments. The senior director of network services and senior network engineers review firewall system logs on an ad hoc basis.	Inquired of the senior network engineer regarding the firewall systems to determine that the senior director of network services and senior network engineers reviewed firewall system logs on an ad hoc basis.	No exceptions noted.
		Inspected the firewall system logging configurations and example firewall system logs generated during the review period for a sample of firewall systems to determine that the firewall systems were configured to log unauthorized remote access attempts to the BHDS environment and client environments for each firewall system sampled.	No exceptions noted.
15.04	Administrator access within the BHDS firewall system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS firewall system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
15.05	Administrator access within the client firewall systems is restricted to user accounts accessible by authorized personnel.	Inspected the firewall system administrator account listings for a sample of client firewall systems with the assistance of the director of strategic services to determine that administrator access within the client firewall systems was restricted to user accounts accessible by authorized personnel for each firewall system sampled.	No exceptions noted.
Vulnerability Assessments			
15.06	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Remote Access		
15.07	Encrypted VPNs are utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	Inquired of a senior network engineer regarding remote network access to client environments to determine that encrypted VPNs were utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	No exceptions noted.
		Inspected the VPN authentication and encryption configurations for a sample of VPN systems to determine that encrypted VPNs were utilized for remote network access to client environments for each VPN system sampled.	No exceptions noted.
15.08	Administrator access within the BHDS VPN system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS VPN system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS VPN system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
15.09	Administrator access within the client VPN systems is restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrator account listings for a sample of client VPN systems with the assistance of the director of strategic services to determine that administrator access within client VPN systems was restricted to user accounts accessible by authorized personnel for each client VPN system sampled.	No exceptions noted.

TRANSITION

Control Objective Specified by the Service Organization: Control activities provide reasonable assurance that risk involved with migrating new client applications to BHDS is mitigated through formal transition planning and multiple validation testing.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
16.01	<p>A project management team is assigned to client application migration projects prior to migration and is responsible for creating the client migration plan that includes, but is not limited to, the following:</p> <ul style="list-style-type: none"> • Timelines and due dates • Tasks and responsibilities • Testing requirements • Client acceptance 	Inquired of the director of strategic services regarding the transition process to determine that a project management team was assigned to client application migration projects prior to migration and was responsible for creating the client migration plan.	No exceptions noted.
		<p>Inspected the project plan for a sample of client application migrations during the review period to determine that a project management team was assigned and that a client migration plan was created for each migration sampled that included the following:</p> <ul style="list-style-type: none"> • Timelines and due dates • Tasks and responsibilities • Testing requirements • Client acceptance 	No exceptions noted.
16.02	<p>Project management personnel provide project status updates via e-mail or conduct project status meetings with client personnel on a weekly basis (unless otherwise specified by the customer) prior to the migration of new client applications.</p>	Inquired of the director of strategic services regarding the transition process to determine that project management personnel provided project status updates via e-mail or conducted project status meetings with client personnel on a weekly basis (unless otherwise specified by the customer) prior to the migration of new client applications.	No exceptions noted.
		<p>Inspected the recurring status updates for a sample of client application migrations during the review period to determine that project management personnel provided project status updates or conducted project status meetings with client personnel on a weekly basis for each client application migration sampled.</p>	No exceptions noted.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
16.03	The project management team requires client personnel to perform multiple stages of validation testing for new client applications prior to migration.	Inquired of the director of strategic services regarding the transition process to determine that the project management team required client personnel to perform multiple stages of validation testing for new client applications prior to migration.	No exceptions noted.
		Inspected the migration ticket for a sample of client application migrations during the review period to determine that client personnel performed validation testing for each client application migration sampled.	No exceptions noted.
16.04	The project management team requires final client approval of new client applications prior to migration.	Inquired of the director of strategic services regarding the transition process to determine that the project management team required final client approval of new client applications prior to migration.	No exceptions noted.
		Inspected the migration ticket for a sample of client application migrations during the review period to determine that final client approval was obtained for each client application migration sampled.	No exceptions noted.



SOC 2 REPORT

FOR

DATA CENTER OUTSOURCING SERVICES

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

MARCH 1, 2021, TO FEBRUARY 28, 2022

Attestation and Compliance Services



This report is intended solely for use by the management of Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services, user entities of Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services' services, and other parties who have sufficient knowledge and understanding of Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services' services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

TABLE OF CONTENTS

SECTION 1	INDEPENDENT SERVICE AUDITOR'S REPORT	1
SECTION 2	MANAGEMENT'S ASSERTION	5
SECTION 3	DESCRIPTION OF THE SYSTEM.....	7
SECTION 4	TESTING MATRICES	23

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services:

Scope

We have examined Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services' ("BHDS" or the "service organization") accompanying description of its Data Center Outsourcing Services system, in Section 3, throughout the period March 1, 2021, to February 28, 2022, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that BHDS's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

BHDS is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that BHDS's service commitments and system requirements were achieved. BHDS has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. BHDS is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;

- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Test of Controls

The specific controls we tested, and the nature, timing, and results of those tests are presented in Section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

- a. the description presents BHDS's Data Center Outsourcing Services system that was designed and implemented throughout the period March 1, 2021, to February 28, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that BHDS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the review period; and
- c. the controls stated in the description operated effectively throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that BHDS's service commitments and system requirements were achieved based on the applicable trust services criteria,

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of BHDS; user entities of BHDS's Data Center Outsourcing Services system during some or all of the period March 1, 2021, to February 28, 2022, business partners of BHDS subject to risks arising from interactions with the Data Center Outsourcing Services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and

- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Columbus, Ohio
April 4, 2022

SECTION 2

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of BHDS's Data Center Outsourcing Services system, in Section 3, throughout the period March 1, 2021, to February 28, 2022, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Data Center Outsourcing Services system that may be useful when assessing the risks arising from interactions with BHDS's system, particularly information about system controls that BHDS has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

We confirm, to the best of our knowledge and belief, that:

- a. the description presents BHDS's Data Center Outsourcing Services system that was designed and implemented throughout the period March 1, 2021, to February 28, 2022, in accordance with the description criteria;
- b. the controls stated in the description were suitably designed throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that BHDS's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and
- c. the controls stated in the description operated effectively throughout the period March 1, 2021, to February 28, 2022, to provide reasonable assurance that BHDS's service commitments and system requirements would be achieved based on the applicable trust services criteria.

SECTION 3

DESCRIPTION OF THE SYSTEM

OVERVIEW OF OPERATIONS

Company Background

Founded in 1994, Computer Technologies U.S.A. LLC d/b/a Blue Hill Data Services (BHDS) is a Tier 2 Information Technology Outsourcing (ITO) infrastructure services provider delivering fully managed, onshore data center hosting solutions and a full array of complementary IT support services to clients worldwide. BHDS specializes in Mainframe, Client Server, and AS/400 iSeries/Mid-Range managed hosting services, colocation services, dedicated high-availability disaster recovery solutions, business continuity solutions, and applications services. BHDS offers mainframe outsourcing solutions, including mainframe migration, mainframe hosting assessment, legacy applications, and software developer hosting. BHDS also provides remote server management options for clients who prefer not to relocate some or all of their servers. In this scenario, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center. The services enable clients to focus on their core business, reduce operating costs, and minimize risk while providing support on a 24 hour per day basis for their business systems. BHDS is headquartered and operates its production data center in Pearl River, New York, with two additional data centers in Branchburg, New Jersey, and Shelton, Connecticut.

Description of Services Provided

Managed Services

The managed services provided by BHDS helps ensure that client environments are proactively managed, and any issues are addressed immediately or eliminated altogether utilizing security monitoring, redundant power, communications, and environmental controls. BHDS provides support on a 24 hour per day basis for Mainframe, AS/400 iSeries/Midrange, and Client Server. Managed services support for the given platforms includes computer operations support, technical support, network support, service desk support, account management, project management, and applications maintenance and support. Services are delivered from BHDS data centers or can be delivered remotely for those clients who wish to have their equipment remain on their premises.

Mainframe Enterprise Server Management

BHDS provides custom configurations of hardware, software, networking, and services in an effort to provide an optimal outsourcing or hosting solutions. Operating environments include z/OS, OS/390, virtual machine (VM), virtual storage extended (VSE), and Linux on the mainframe. BHDS Mainframe enterprise server management support services include technical services/systems support, computer operations support, production control / job scheduling, network support, service desk, and account management.

Client Server Tools

With the ability to monitor database parameters and e-mail tasks in products such as SQL, Oracle, Exchange, Lotus Notes, etc., BHDS's Client Server monitoring helps ensure that servers are running smoothly and maximizing their availability and performance. BHDS's Client Server advanced management tools, including monitoring and alerting software, remote management capabilities, and backup and recovery software. BHDS is particularly active in virtualization of client server images for clients and utilizes VMware as the standard for virtualization of multiple server images onto large complex server footprints to deliver value and performance to clients. These Client Server tools automatically monitor server health, provide diagnostics, backup and restore data, and repair server issues. BHDS also hosts several UNIX server platforms (Advanced Interactive Executive (AIX), Solaris, Hewlett-Packard Unix (HP-UX), Linux), as well as provides remote server management options for clients who prefer not to relocate some or all of their servers. In this case, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center.

AS/400 iSeries/Midrange Management

BHDS provides hosting and support services for Midrange Servers including continuous server alert monitoring and an expert support team to help ensure issues are prevented from occurring before they impact a client's systems or their user community. BHDS also provides remote server management options for clients who prefer not to relocate some or all of their servers. In this case, some or all of the servers remain at the client's site but are managed by BHDS staff from their central operations center.

Network Services

The BHDS network support team works with clients to design and support the local area and global data networks. BHDS enforces the client's TCP/IP standards and helps ensure that these standards are strictly adhered to. The Network Support team provides consulting and support services to clients for various IT projects involving infrastructure, security, access, and network standards. BHDS helps ensure that bandwidth is sufficient by monitoring network data traffic. The Network Support team provides proactive analysis required to help ensure peak performance of wide area network (WAN) infrastructure, and to maintain physical network maps showing network devices in the environment. They also monitor the VPN and network environment located in the data center. In addition, the Network Support team monitors clients' networks by reporting outages and key performance statistics. If an outage occurs and is circuit related, the Network Support team immediately addresses the system outage, monitors the status of the routers at each location, and notifies the given carriers. If the outage is equipment related, the client is responsible for working with their respective hardware vendors, and once the hardware is repaired, BHDS will work with the client to re-establish network connectivity.

Service Desk Services

BHDS provides robust service desk services 24x7x365 for their offerings and platforms. The service desk serves as a single point of contact by phone call or e-mail for clients and support staff. The service desk analyst proactively works to resolve requests and issues upon initial contact, and coordinates escalation and follow-up with support teams. BHDS utilizes a full featured, multi-client service desk application called information Service Desk Management System (iSDMS) to track problems, change requests, and service requests for BHDS clients. The secure cloud-based application documents related information and provides extensive search and reporting capabilities. iSDMS includes a fully customizable automated client interface that allows for the synchronization of tickets between iSDMS and the customers own service desk system. In addition, a web-based portal is available 24x7 to clients for secure self-serve access to their tickets and information.

Data Center

The production data center facility located in Pearl River, New York, covers more than 100,000 square feet including 65,000 square feet of raised floor space.

Multi-Layered Security

- Security guard station and sign-in desk for visitors at the main entrance of the building staffed on a 24 hour per day basis.
- Security guard station and sign-in desk is located outside the computer room entrance.
- Data center command station equipped with digitally recorded, continuous video surveillance cameras monitored by personnel on a 24 hour per day basis.
- Video feeds monitoring data center egress and ingress points, loading dock, colocation areas, and backup facilities.
- Multiple closed-circuit television time-lapse cameras located throughout the facility and data center.
- Badge access card system throughout the facility to control access into and throughout the facility.
- Data center visitors required to be escorted by BHDS personnel into and throughout the data center.

Redundancy

- Underground dual redundant power feeds directly from the Northeast power grid via dual diverse paths from local utility's primary transmission network.
- Diesel power generators configured with automatic transfer switches in the event of a primary power source failure.
- Uninterrupted power supply (UPS) systems in place.
- Redundant power distribution panels feed to server racks and stand-alone equipment.
- Dual redundant communications access provided by Verizon from two separate entry points into the BHDS complex.

- Tertiary diverse internet service providers (ISPs) are Internap Network Services (Internap NY PNAP, Internap NJ PNAP), Lightpath (Altice), and Crown Castle.
- Verizon Business, Verizon Core, Optimum Lightpath, and Crown Castle provide direct fiber feeds into the data center facility.
- Point-to-point Metro Ethernet connectivity directly from the data center facility to the New York Tri-State area network to provide high availability and high-capacity data transfer capabilities.
- Fully redundant ingress and egress internet access provided by Border Gateway Protocol across providers.

Environmental

- Multiple energy efficient humidification and temperature air handling systems.
- Ten 20-ton and one 12-ton Liebert computer room air-conditioning (CRAC) units in an N+1 or N+2 configuration.
- Centralized monitoring of the fire alarm system provided by building security.
- Double Interlock fire detection and suppression systems.
- Pre-action fire suppression, cross-zoned system, smoke and heat detection sensors, and hand-held fire extinguishers.
- FireSystems environmental monitoring tool to alert personnel of evacuation.
- Environmental systems monitored on a 24 hour per day basis by the central command center.
- Fault tolerant facility with a certified lightening protection system and complete building grounding system.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

BHDS designs its processes and procedures related to the Data Center Outsourcing Services system to meet its objectives for its Data Center Outsourcing services. Those objectives are based on the service commitments that BHDS makes to user entities, the laws and regulations that govern the provision of the Data Center Outsourcing Services system, and the financial, operational, and compliance requirements that BHDS has established for the services. The Data Center Outsourcing Services system of BHDS is subject to the relevant regulatory and industry information and data security requirements in which BHDS operates.

Security and availability commitments to user entities are documented and communicated in service level agreements (SLAs), statements of work (SOW), and other customer agreements, as well as in the description of the service offering provided online.

The principal security and availability commitments are standardized and include, but are not limited to, the following:

- Maintenance of a disaster recovery program;
- 24/7/365 system access;
- Physical, administrative, and technical safeguards for associated hardware within the data center;
- The use of logical access controls to protect against unauthorized access and security breaches; and
- Implementation of security measures to safeguard the network and client data.

BHDS establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. BHDS maintains an information security program that includes, but is not limited to, ongoing employee training for information security practices, the use of encryption to protect data, the use of firewalls to protect against unauthorized network traffic, testing and updating the disaster recovery plan on an annual basis, restricting access to authorized personnel, and performing client data backups.

Such requirements are communicated in BHDS's system policies and procedures, trainings, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired, trained, and managed. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Data Center Outsourcing services.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICE

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

BHDS uses multiple tools to capture, record, and address system events. BHDS monitors its clients' systems using both real-time monitoring tools, as well as historical trend reporting tools. The iSDMS support desk ticketing system captures events related to incidents, changes, or asset management. The iSDMS support desk ticketing system is a custom-built system that interfaces with a client's specific service desk system.

The in-scope infrastructure consists of systems and platforms as shown in the table below:

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Network Domain	Microsoft Active Directory network domain controller that manages the operating system servers.	Windows	Data Center – Pearl River, NY
VPN	Authenticates and authorizes the organization's employees accessing the production network.		
Production Servers	Mainframe, AS/400 iSeries/Midrange, and Client Server ISM servers and related services.	Mainframe, AS/400 iSeries/Midrange, and ISM	
Firewall Systems	Firewalls provide the ability to configure, control, and restrict inbound and outbound network traffic into the production infrastructure within the managed environment.	Windows	
Intrusion Detection System (IDS)	Cisco Network IDS analyzes network events for possible or actual security breaches and alert management.		

Primary Infrastructure			
Production System	Business Function Description	Platform	Physical Location
Environmental Monitoring Tool	FireSystems environmental monitoring tool is in place to alert personnel of environmental issues and is monitored on a 24 hour per day basis by the central command center.	Windows	Data Center – Pearl River, NY
Enterprise Monitoring Tools	<p>iSDMS - captures and reports on problem, change, and asset management events.</p> <p>I/O Concepts ioEnterprise Event Manager and Smart Client – captures mainframe system events and manages error messages.</p> <p>RevSoft Enterprise Solution Suite – utilized for monitoring and reporting of AS/400 iSeries Midrange environments.</p> <p>SolarWinds Orion and Site 24X7 – monitors open system environments and gives alerts on failed processes or connections.</p> <p>Ipswitch WhatsUp Gold IP Monitor – utilized to monitor infrastructure and network environments, alerts on failed processes or connections.</p>		

People

The personnel supporting the Data Center Outsourcing Services system include, but are not limited to, the following:

- Executive management – responsible for organizing and overseeing activities, accomplishing goals, and overseeing objectives in an efficient and effective manner.
- Data center operation – responsible for managing and maintaining the command center, consoles, systems, production control / job scheduling, and service desk support for user entities on a 24 hour per day basis.
- Systems administration – responsible for specifying, deploying, and maintaining infrastructure systems, security and availability, and technical support for user entities.
- Network engineering – responsible for specifying, deploying, and maintaining network infrastructure, security and availability, and support for user entities.
- Facilities and building engineering – responsible for managing and protecting the physical security, environmental, electrical, and physical integrity of the building.

Procedures

Access, Authentication and Authorization

In order to access the managed environment, users must first be provisioned with VPN access. VPN sessions are encrypted via TLS and require two-factor authentication requiring a user account, personal identification number (PIN) code, and Rivest-Shamir-Adleman (RSA) SecurID token. Remote access to managed environments is restricted to user accounts accessible by authorized personnel.

Upon successful authentication via the VPN system, users can authenticate to the managed infrastructure via a user account and password. The managed network is configured to enforce password requirements that include minimum length, expiration intervals, complexity requirements, minimum history, and invalid account lockout

threshold. Once in the managed infrastructure, users can access client systems. Administrator access within the client systems is restricted to user accounts accessible by authorized personnel.

The managed network is configured to log the following events for ad hoc and scheduled review purposes: account logon events, account management events, directory service access events, logon events, policy changes, and system events. Technical services personnel review these logs on an ad hoc and scheduled basis to determine if any suspicious or unauthorized activity has occurred. In the event any suspicious or unauthorized activity occurred within the managed network, technical services personnel would investigate and follow-up for resolution.

Clients operating in a shared environment are logically segmented to help ensure confidentiality of client's data. In addition, Open System clients run on dedicated and physically separate processing environments. Furthermore, Open System clients utilizing shared storage area network (SAN) disk storage are segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments.

Access Requests and Access Revocation

A formal process has been established to manage user access requests, modifications, and deletions. When a new employee is hired that requires remote access to client system, an account manager submits e-mail notifications to each applicable client representative requesting access for the new employee. Technical services personnel are also copied on the e-mail notifications. Upon approval from each applicable client representative, technical services personnel provision access for the new employee based on specified requirements noted in the e-mail notifications.

Client representatives request modification of client user account access privileges via e-mail or verbal correspondence with a member of client services. Once a client representative submits the request, a member of client services will log it into the iSDMS support desk ticketing system. Client services personnel log key fields within the ticket, including the client name, contact name, system, and description. Upon the creation of a ticket, client services personnel route the ticket to an operator, systems engineer, or systems administrator and the requested modifications are processed based upon the ticket. Once the requested modifications are complete, client services personnel close the ticket and notify the client representative via e-mail.

Upon notification of an employee termination from the hiring manager, technical services personnel disable the employee's VPN access to managed infrastructure. Human Resources (HR) personnel complete a termination checklist in conjunction with the removal of access. The termination checklist is maintained within the personnel file for documentation purposes.

Physical Security

When a new hire requires physical access to the office suite, the hiring manager completes a new employee user setup form to authorize access and submits it to the service desk via e-mail. Upon notification, the service desk opens a service desk ticket requesting that a badge access card be created for the new employee. The service desk then forwards the service desk ticket to the chief facilities engineer via e-mail. Upon notification, the chief facilities engineer activates a badge access card for issuance to the employee by HR. HR also completes a new hire checklist to document that the new employee received a badge access card.

In the instance that an employee is terminated, the executive office manager or terminated employee's direct supervisor completes a termination form and submits it to the service desk via e-mail. Upon notification, the service desk opens up a service desk ticket requesting that the terminated employee's badge access card be disabled. The service desk then forwards the service desk ticket to the chief facilities engineer via e-mail. Upon notification, the chief facilities engineer disables the terminated employee's badge access card. HR retrieves the terminated employee's badge access card during the employee's exit interview and completes a termination checklist in conjunction with the retrieval of the badge access card.

A badge access system is utilized to control access to the office suite. The badge access system utilizes pre-defined access zones so that certain areas of the office suite remain restricted. Furthermore, the badge system maintains a log of activity, allowing facilities and building engineering personnel the ability to trace access attempts to specific badges. Facilities and building engineering personnel review badge access system logs on an ad hoc and scheduled basis. Administrator access within the badge access system (i.e., the ability to add, modify, and revoke access privileges) is restricted to authorized personnel.

Badge access privileges assigned to terminated employees are revoked as a component of the employee termination process. In the instance that an employee is terminated, the executive office manager or terminated employee's direct supervisor completes a termination form and submits it to the service desk via e-mail. Upon notification, the service desk opens a service desk ticket requesting that the terminated employee's badge access card be disabled. The service desk then forwards the service desk ticket to the chief facilities engineer via e-mail. Upon notification, the chief facilities engineer disables the terminated employee's badge access card. HR retrieves the terminated employee's badge access card during the employee's exit interview and completes a termination checklist in conjunction with the retrieval of the badge access card. On a monthly basis, the account manager reviews badge access privileges within the office suite and data center to help ensure that badge access privileges are authorized for each employee. In the event that unauthorized access is discovered, it is corrected, investigated, and documented within the results of the review.

Production infrastructure is located within a secure data center in locked cabinets; data center personnel maintain a list of production infrastructure that is secured within the cabinets of the data center. The ability to access the data center is restricted via the badge access system. Furthermore, the badge system maintains a log of activity that is traceable to specific badge access cards, allowing facilities and building engineering personnel the ability to trace access attempts to specific badges by reviewing the logs on an ad hoc and scheduled basis.

Visitors are required to sign a visitor log upon entry into the data center. Within the visitor log, visitors document their name, date, company, and time in. While within the data center, visitors are required to be escorted by a member of facilities or operations.

Digital surveillance cameras are in place to monitor and record activity at the entrance to and throughout the data center. The digital surveillance cameras retain images/recordings for a minimum of three months.

The processes for provisioning and revoking badge access privileges for the data center follows the standard office suite processes as described above. Access to the data center is restricted to authorized personnel. Data center walls extend from the real floor to the real ceiling restricting physical access to the data center.

A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media. Property pass forms are utilized to document the removal of equipment from the data center. The chief facilities engineer, or account manager is responsible for approving property pass forms.

Network Security

Multiple firewall systems are in place and utilized to protect the production environment and data including filtering unauthorized inbound network traffic from the internet. External internet traffic is required to pass through the firewalls to communicate with the production servers. Any type of connection that is not explicitly authorized by the firewalls will be denied. The firewall systems are configured to log unauthorized remote access attempts to the BHDS environment and client environments. The senior director of network services and senior network engineers review firewall system logs on an ad hoc and scheduled basis to identify suspicious activity and abnormal connection attempts. In the event of an invalid login attempt, the senior director of network services and senior engineers would remove the offending subnet from the ISP routers. Administrator access within the client and BHDS firewall systems is restricted to authorized personnel.

A third-party specialist is utilized to perform external vulnerability scans of the production network to identify potential security vulnerabilities on a monthly basis. Operations management retains the assessment report, monitors the results of the assessment within the report, and creates remediation plans to remedy any potential vulnerabilities.

Encrypted VPNs are utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network. Access to managed infrastructure is secured via an encrypted VPN that requires two factor authentication using RSA SecurID technology that includes having a user account, PIN, and individual token generator. Administrator access within the client and BHDS VPN systems is restricted to authorized personnel.

Antivirus

The antivirus solution is configured to protect registered production servers and workstations to scan for updates to antirust definitions and update registered clients on a continuous basis through a cloud-based service. Registered servers and workstations are scanned on a continuous basis.

Change Management

Documented procedures are in place to help guide the BHDS and client change management process. BHDS management and engineers hold monthly change management meetings to discuss and notify management personnel of upcoming changes and ongoing projects that affect the system. Change requests are initiated by BHDS or a BHDS client via e-mail and contain general information about the change proposal. The change is reviewed, approved, and tracked in the service desk ticketing system to centrally maintain, manage, monitor upgrades and maintenance activities, and client system change requests. Change tickets include a description of change, estimated impact, and assignment of a change manager. For changes that require testing, operations management require client personnel to perform user acceptance testing (UAT) for upgrades prior to implementation, as well as provide final approval prior to implementation. BHDS has limited the ability to implement server upgrades within client managed environments to authorized personnel.

Emergency changes may be required to restore service or prevent an impending outage situation. In these instances, clients and Blue Hill management are notified as soon as possible and a ticket will be created to follow the standard change management process.

Data Backup and Disaster Recovery

Documented SLAs that define backup and recovery services for clients are in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions. Multiple backup systems are utilized to perform backups of client data according to specifications documented in the SLA. Operations personnel monitor the status of backup processing on a 24 hour per day basis. Processing errors are reported to technical personnel for resolution and documented in a service desk ticket. A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media. Operations personnel rotate backup media to the off-site third-party media vaulting company on a daily, weekly, and monthly basis in accordance with client specifications. Operations personnel maintain backup and recovery procedures for clients subscribed to hot-site services and are tested according to client requirements.

Disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. Disaster recovery plans are tested on at least an annual basis.

Environmental Security

The equipment in the data center is connected to UPS to provide temporary electricity in the event of a power outage and mitigate the risk of power surges impacting infrastructure. The data center is also equipped with generators to provide electricity in the event of a power outage. For temperature control, air conditioning units are in place within the data center to regulate temperature. Fire detection and suppression equipment are also in place in the event of a data center fire. The environmental protection equipment are reviewed by a third party on an annual basis.

System Monitoring

Multiple enterprise monitoring applications are utilized to monitor the health and availability of the overall production environment. In the event that a component of the monitored environment falls out of the pre-defined monitoring thresholds configured within the systems, the enterprise monitoring applications are configured to notify operations personnel via e-mail in real-time. Once notified, operations personnel review the alerts and investigate the cause. A network engineer obtains the third-party external vulnerability scan reports as evidence that external vulnerability scans of the production network are performed on a monthly basis. Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.

An IDS is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches. Multiple firewall systems are in place and utilized to protect the production environment and data. External internet traffic is required to pass through the firewalls to communicate with the production servers. Any type of connection that is not explicitly authorized by the firewalls will be denied. The firewall systems are configured to log unauthorized remote access attempts to the BHDS environment and client environments. The senior director of network services and senior network engineers review firewall system logs on an ad hoc and scheduled basis to identify suspicious activity and abnormal connection attempts. In the event of an invalid logon attempt, the senior director of network services and

senior engineers would remove the offending subnet from the ISP routers. Administrator access within the client and BHDS firewall systems is restricted to authorized personnel.

Incident Response

Incident response procedures are in place that outline the response procedures to security events and includes lessons learned to evaluate the effectiveness of the procedures. Documented computer operations procedures are in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties. An automated ticketing system is utilized to prioritize, log, and track resolution steps for service requests and incidents. Additionally, a standard operating procedure (SOP) for incident notification, escalation, and resolution is provided to personnel. Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure. In the event that a component of the monitored environment falls out of the predefined monitoring thresholds configured within the system, the enterprise monitoring applications are configured to notify operations personnel via e-mail in real-time. Once notified, operations personnel review the alerts and investigate the cause. A maintenance and service agreement is in place with an ISP to provide coverage for communications components on a 24 hour per day basis.

Data

BHDS uses multiple tools to capture, record, and address system events. BHDS monitors its clients' systems using both real-time monitoring tools, as well as historical trend reporting tools. The iSDMS support desk ticketing system captures events related to incidents, changes, or asset management. The iSDMS support desk ticketing system is a custom-built system that interfaces with a client's specific service desk system.

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
System events	Alerting and notification of environments / support desk tickets and incidents.	Sensitive
System performance	Metrics on system environment / availability.	

Significant Changes During the Review Period

There were no significant changes that are likely to affect report users' understanding of how the in-scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

No subservice organizations were relevant to the scope of this assessment whose controls were necessary, in combination with controls at BHDS, to provide reasonable assurance that [insert service organization abbreviated name]'s service commitments and system requirements were achieved.

CONTROL ENVIRONMENT

The control environment at BHDS is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational

structure; the assignment of authority and responsibility; and the oversight and direction provided by executive management and operations management.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of BHDS's control environment, affecting the design, development, administration, and monitoring of other components. Integrity and ethical behavior are the product of BHDS's ethical and behavioral standards, how they are communicated and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations to that might prompt personnel to engage in dishonest, illegal, and unethical behavior. Specific control activities that BHDS has implemented in this area are:

- Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.
- Employees are required to sign a confidentiality agreement on an annual basis agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- New employees are required to attend a new hire orientation session as a component of the hiring process to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.
- New employees are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.
- HR personnel perform background checks for job candidates who are extended an offer of employment as a component of the hiring process.
- HR personnel require contractors to submit to a background check prior to being engaged as a contractor.
- An employee sanction procedure is in place and documented within the code of conduct communicating that an employee may be terminated for noncompliance with a policy or procedure.

Executive Management Committee Oversight

BHDS's control consciousness is influenced significantly by its executive management team. The team is comprised of experienced individuals who oversee day-to-day activities and conducts meetings to discuss matters pertinent to the organization's operational and business objectives. An executive management meeting is held on a weekly basis to discuss the performance and function of internal controls. Management holds an annual strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.

Organizational Structure and Assignment of Authority and Responsibility

BHDS's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Establishing an organizational structure include considering key areas of authority, responsibility, and lines of reporting. BHDS's organizational structure is suited to support its strategic objectives and its customers. The appropriateness of BHDS's organizational structure depends, in part, on its size and the nature of its activities.

This factor includes how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to business practices, knowledge and experience of key personnel, and resources provided for carrying out job responsibilities. Policies and communications are directed at helping ensure that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that BHDS has implemented in this area are described below.

- Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.
- Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.
- An executive management team comprised of security personnel has been established to guide the company in managing security and availability risks.

Commitment to Competence

BHDS defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge. BHDS's HR policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating, and remedial actions. For example, standards for hiring the most qualified individuals include emphasis on educational background, prior work experience, past accomplishments, and evidence of integrity and ethical behavior. Promotions driven by periodic performance appraisals demonstrate BHDS's commitment to the advancement of qualified personnel to higher levels of responsibility. In addition to position descriptions, specific controls that BHDS has implemented in this area are described below.

- New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.
- HR personnel perform screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process.
- Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.
- Hiring managers perform employee performance evaluations on an annual basis.
- Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.
- Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.

Accountability

Management personnel establish accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. In addition to formal job descriptions and annual performance reviews, specific control activities that BHDS has implemented in this area are described below.

- Management holds an annual strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.
- An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.

RISK ASSESSMENT

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and confidentiality categories.

Objective Setting

The risk assessment process involves a dynamic process that includes identification and analyzation of risks that pose a threat the organization's ability to perform the in-scope services. The process starts with determining the organization's objectives as these objectives are key to understanding the risks and allows identification and analyzation of those risks relative to the objectives. Management then holds an annual strategy meeting that discusses and aligns internal control responsibilities, performance measures and incentives with company business objectives.

Risk Identification and Analysis

BHDS has considered significant interactions between itself and relevant external parties and risks that could affect the organization's ability to provide reliable service to its user entities. To help identify risk, documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process. Security stakeholders perform a risk assessment on an annual basis that identifies and analyzes the business, security risks, and vulnerabilities, laws, and regulations. Risks identified are formally documented, along with mitigation strategies, and reviewed by management. The risk assessment also considers the impact of changes to the system. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities
- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing

- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

A documented policy and procedure is in place to guide personnel in identifying the potential for fraud as part of the risk assessment process. A formal risk assessment is performed on an annual basis that considers the potential for fraud in assessing risks to the achievement of objectives.

Risk Mitigation

Risk mitigation activities include the ability to identify, select, and develop activities that sufficiently mitigate the identified risks to acceptable levels. However, the relative costs versus benefits should also be considered when determining the risk mitigation activities. Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies based on identified risks and vulnerabilities. Treatment and mitigation plans are developed based on risk evaluation performed. The annual risk assessment also includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions. To further reduce risk, BHDS utilizes a cyber reliability insurance policy that would allow for continued support to return to successful business operations if an impactful cybersecurity disruption occurred.

In addition, vendor management policies and procedures are in place to guide personnel in assessing and managing risks associated with third parties. Vendor risks are considered as a component of the annual risk assessment and includes mitigation control activities for risks arising from vendor risks.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability categories.

Selection and Development of Control Activities

Selecting control activities includes consideration of the relevant processes and identified risks that require control activities. Both automated and manual controls are considered during the selection of control activities. Documented policies and procedures are in place to help guide personnel in selecting and developing control activities that contribute to the mitigation of risks when performing the risk assessment process. On an annual basis, security stakeholders perform a risk assessment that includes an analysis of risk mitigation control activities and considers how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities. As part of this process, risk owners select and develop control activities to mitigate the risks as well as control activities over technology to support the achievement of objectives as an output identified during the annual risk assessment process. The corresponding control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.

Control activities are deployed through the use of information security and operating policies to establish what is expected and procedures that put policies into action. Employees are held accountable for compliance with company policies where an employee sanction policy is in place to address remedial action for noncompliance with a policy and/or procedure. These policies and procedures are communicated to internal personnel via the intranet.

The applicable trust services criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust services criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of BHDS's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security and availability categories are applicable to the Data Center Outsourcing Services system.

INFORMATION AND COMMUNICATION SYSTEMS

Pertinent information must be identified, captured, and communicated in a form and timeframe that enable people to carry out their responsibilities. Information systems produce reports, containing operational, financial, and compliance-related information, that make it possible to run and control the business. They deal not only with internally generated data, but also information about external events, activities, and conditions necessary to inform business decision-making and external reporting. Effective communication also must occur in a broader sense, flowing down, across and up the organization. Personnel must receive a clear message from top management that control responsibilities must be taken seriously. They must understand their own role in the internal control system, as well as how individual activities relate to the work of others. They must have a means of communicating significant information upstream. There also needs to be effective communication with external parties, such as customers, suppliers, regulators, and shareholders.

Internal Communications

BHDS has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. Communication takes such forms as policy manuals, memorandums, and trainings. Communications also can be made electronically, verbally, and through the actions of management. When applicable, BHDS has implemented various methods of communication to help provide assurance that employees understand their individual roles and responsibilities and that significant events are communicated. These methods include having documented position descriptions, incident response procedures, and notification procedures for ongoing and upcoming projects.

External Communications

BHDS has also implemented various methods of communication to help provide assurance that customers understand the roles and responsibilities in processing their transactions and communication of significant events. These methods include having a system product description available to user entities on the Blue Hill Managed Services site and documented security and availability commitments and associated system requirements in customer contracts and SLAs. Service requests and incidents with potential impact to security and availability commitments are logged, reported, and communicated by operations personnel to clients through e-mail as specified by the SLA. In addition, BHDS has a phone hotline and service desk e-mail address available to external users to report security or availability failures, incidents, and other complaints.

MONITORING

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented a self-assessment and compliance program to ensure the controls are consistently applied as designed.

Ongoing Monitoring

By monitoring the risks and the effectiveness of control measures on a regular basis, BHDS can react dynamically to changing conditions. Enterprise monitoring applications are utilized to monitor processing activities for exceptions and anomalies and configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded, or controlled events are triggered. Additional tools are in place, such as an IDS, which is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches.

Separate Evaluations

Evaluation of an entire internal control system may be prompted by a number of reasons: major strategy or management change, major acquisitions or dispositions, or significant changes in operations or methods of processing information. Evaluations of internal control vary in scope and frequency, depending on the significance of risks being controlled and importance of the controls in reducing the risks. Controls addressing higher-priority risks and those most essential to reducing a given risk will tend to be evaluated more often. BHDS has processes in place where a network engineer obtains the third-party external vulnerability scan reports as evidence that external vulnerability scans of the production network are performed on a monthly basis. Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.

Evaluating and Communicating Deficiencies

Management has developed protocols to help ensure findings of internal control deficiencies are reported to the individuals responsible for the function or activity involved and are in the position to take corrective action. This process enables responsible individuals to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities. External vulnerability scans are performed on a monthly basis whereby the security operations and infrastructure team then track, review, and remediate security vulnerabilities identified according to security remediation standards. The entity's information technology security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.

System Incident Disclosures

No system incidents occurred that were the result of controls that were not suitably designed or otherwise resulted in a significant failure of the achievement of one or more of the service commitments and systems requirements.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Data Center Outsourcing Services system provided by BHDS. The scope of the testing was restricted to the Data Center Outsourcing Services system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period March 1, 2021, to February 28, 2022.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employee manual and understand their responsibility for adhering to the code of conduct outlined within the manual.	Inspected the acknowledgement forms for a sample of employees hired during the review period to determine that employees were required to sign an acknowledgment form upon hire indicating that they had been given access to the employee manual and understood their responsibility for adhering to the code of conduct outlined within the manual for each employee sampled.	No exceptions noted.
CC1.1.2	New employees are required to attend a new hire orientation session as a component of the hiring process to help ensure that they are familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.	Inquired of the director of office administration regarding the hiring process to determine that new employees were required to attend a new hire orientation session as a component of the hiring process to help ensure that they were familiar with company operations, standards of conduct, confidentiality requirements, conflicts of interest, and other operating policies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of new hire orientation session attendance for a sample of employees hired during the review period to determine that new employees attended a new hire orientation session as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.3	New employees and contractors are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreements for a sample of employees and contractors hired during the review period to determine that new employees and contractors were required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties for each employee and contractor sampled.	No exceptions noted.
CC1.1.4	Employees are required to sign a confidentiality agreement on an annual basis agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreements for a sample of current employees to determine that employees were required to sign a confidentiality agreement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties during the review period for each employee sampled.	No exceptions noted.
CC1.1.5	HR personnel perform background checks for job candidates who are extended an offer of employment as a component of the hiring process.	Inspected evidence of background check performance for a sample of employees hired during the review period to determine that HR personnel performed background checks for job candidates who were extended an offer of employment as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.1.6	HR personnel require contractors to submit to a background check as a component of the contract engagement process.	Inspected evidence of background check completion for a sample of contractors hired during the review period to determine that HR personnel performed required contractors to submit to a background check as a component of the engagement process for each contractor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.7	An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	Inspected the employee handbook procedures to determine that an employee sanction procedure was in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	An executive management team comprised of security personnel has been established to guide the company in managing security and availability risks.	Inquired of the director of strategic services regarding the executive management team to determine that a group comprised of security personnel was established to guide the company in managing security and availability risks.	No exceptions noted.
		Inspected the organizational chart to determine that an executive management team was comprised of security personnel.	No exceptions noted.
CC1.2.2	Management holds a strategy meeting on at least an annual basis that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the meeting invite, attendees, and meeting minutes from the strategy meeting to determine that management held a strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives during the review period.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.	Inquired of the director of office administration regarding organizational charts to determine that organizational charts were in place to communicate key areas of authority and responsibility and that the charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organizational chart to determine that organizational charts were in place and identified key areas of authority and responsibility.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.3.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each employee sampled.	No exceptions noted.
CC1.3.3	An executive management team comprised of security personnel has been established to guide the company in managing security and availability risks.	Inquired of the director of strategic services regarding the executive management team to determine that a group comprised of security personnel was established to guide the company in managing security and availability risks.	No exceptions noted.
		Inspected the organizational chart to determine that an executive management team was comprised of security personnel.	No exceptions noted.
CC1.3.4	Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.	Inquired of the director of office administration regarding manager practices to determine that managers were actively involved in supervising and reviewing the work of subordinate employees and were responsible for helping to ensure compliance to client and company operating procedures.	No exceptions noted.
		Inspected the business process procedures to determine that managers were actively involved in supervising and reviewing the work of subordinate employees.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each employee sampled.	No exceptions noted.
CC1.4.2	New employee hiring procedures are in place to guide the hiring process and include verification that candidates possess the required qualifications to perform the duties as outlined in the job description.	Inspected the new employee hiring procedures to determine that new employee hiring procedures were in place to guide the hiring process and included verification that candidates possessed the required qualifications to perform the duties as outlined in the job description.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.3	HR personnel perform screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process.	Inquired of the director of office administration regarding the hiring process to determine that HR personnel performed screening and evaluation of job candidates in accordance with job descriptions.	No exceptions noted.
		Inspected evidence of screening and evaluation for a sample of employees hired during the review period to determine that HR personnel performed screening and evaluation of job candidates in accordance with job descriptions as a component of the hiring process for each employee sampled.	No exceptions noted.
CC1.4.4	Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.	Inquired of the director of office administration regarding the hiring process to determine that hiring managers evaluated new employees after a 90-day probation period to help ensure that they were able to sufficiently perform the duties associated with their job function.	No exceptions noted.
		Inspected the 90-day evaluations for a sample of employees hired during the review period to determine that a hiring manager completed an evaluation after the 90-day probation period for each employee sampled.	No exceptions noted.
CC1.4.5	Hiring managers perform employee performance evaluations on an annual basis.	Inspected the employee performance evaluations for a sample of current employees to determine that hiring managers performed employee performance evaluations during the review period for each employee sampled.	No exceptions noted.
CC1.4.6	Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.	Inquired of the director of office administration regarding security awareness training to determine that employees were required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.	No exceptions noted.
		Inspected the security awareness training materials and completion documentation for a sample of current employees to determine that security awareness training was completed during the review period for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.7	Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.	Inquired of the director of office administration regarding manager practices to determine that managers were actively involved in supervising and reviewing the work of subordinate employees and were responsible for helping to ensure compliance to client and company operating procedures.	No exceptions noted.
		Inspected the business process procedures to determine that managers were actively involved in supervising and reviewing the work of subordinate employees.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Documented business process procedures are in place to guide personnel in key business processes including, but not limited to, the following: <ul style="list-style-type: none">• HR• Payroll• Procurement• Revenue recognition and deferred accounting	Inspected the business process procedures to determine that documented business process procedures were in place to guide personnel in key business processes that included the following: <ul style="list-style-type: none">• HR• Payroll• Procurement• Revenue recognition and deferred accounting	No exceptions noted.
CC1.5.2	Organizational charts are in place to communicate key areas of authority and responsibility. These charts are communicated to employees and updated as needed.	Inquired of the director of office administration regarding organizational charts to determine that organizational charts were in place to communicate key areas of authority and responsibility and that the charts were communicated to employees and updated as needed.	No exceptions noted.
		Inspected the organizational chart to determine that organizational charts were in place and identified key areas of authority and responsibility.	No exceptions noted.
CC1.5.3	Management holds a strategy meeting on at least an annual basis that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the meeting invite, attendees, and meeting minutes from the strategy meeting to determine that management held a strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.4	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each employee sampled.	No exceptions noted.
CC1.5.5	Hiring managers evaluate new employees after a 90-day probation period to help ensure that they are able to sufficiently perform the duties associated with their job function.	Inquired of the director of office administration regarding the hiring process to determine that hiring managers evaluated new employees after a 90-day probation period to help ensure that they were able to sufficiently perform the duties associated with their job function.	No exceptions noted.
		Inspected the 90-day evaluations for a sample of employees hired during the review period to determine that a hiring manager completed an evaluation after the 90-day probation period for each employee sampled.	No exceptions noted.
CC1.5.6	Hiring managers perform employee performance evaluations on an annual basis.	Inspected the employee performance evaluations for a sample of current employees to determine that hiring managers performed employee performance evaluations during the review period for each employee sampled.	No exceptions noted.
CC1.5.7	An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	Inspected the employee handbook procedures to determine that an employee sanction procedure was in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Information security policies and procedures are in place to guide personnel in the entity's security practices and are communicated to personnel via the company intranet.	Inspected the security policies on the company intranet to determine that information security policies and procedures were in place to guide personnel in the entity's security practices and were communicated to personnel via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.2	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC2.1.3	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.
CC2.1.4	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the director of strategic services regarding third-party security updates to determine that the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected an example security update e-mail from a third-party to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
CC2.1.5	Enterprise monitoring applications are utilized to monitor processing activities for exceptions and anomalies.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor processing activities for exceptions and anomalies.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.6	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded, or controlled events are triggered.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded, or controlled events were triggered.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Employees are required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.	Inquired of the director of office administration regarding security awareness training to determine that employees were required to complete security awareness training on an annual basis to understand their obligations and responsibilities to comply with the organization's security policies.	No exceptions noted.
		Inspected the security awareness training materials and completion documentation for a sample of current employees to determine that security awareness training was completed during the review period for each employee sampled.	No exceptions noted.
CC2.2.2	Documented position descriptions are in place to define the skills, responsibilities, and knowledge levels required for particular jobs.	Inspected the position descriptions for a sample of employees hired during the review period to determine that documented position descriptions were in place to define the skills, responsibilities, and knowledge levels required for particular jobs for each employee sampled.	No exceptions noted.
CC2.2.3	Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities.	Inspected the incident response procedures to determine that documented incident response procedures were in place to guide personnel in server and network outage response, escalation, and resolution activities.	No exceptions noted.
CC2.2.4	BHDS management and engineers are notified of changes and ongoing and upcoming projects that affect the system via monthly change management meetings.	Inquired of the director of strategic services regarding change management meetings to determine that BHDS management and engineers were notified of changes and ongoing and upcoming projects that affected the system via monthly change management meetings.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the recurring change management calendar invite to determine that BHDS management and engineers were notified of changes and ongoing and upcoming projects that affected the system via the monthly change management meetings.	No exceptions noted.
CC2.2.5	Information security policies and procedures are in place to guide personnel in the entity's security practices and are communicated to personnel via the company intranet.	Inspected the security policies on the company intranet to determine that information security policies and procedures were in place to guide personnel in the entity's security practices and were communicated to personnel via the company intranet.	No exceptions noted.
CC2.2.6	Management holds a strategy meeting on at least an annual basis that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the meeting invite, attendees, and meeting minutes from the strategy meeting to determine that management held a strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives during the review period.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The system and product description is documented and available to user entities on the Blue Hill Managed Services site.	Inspected the managed services website to determine that the system and product description was documented and was available to user entities on the Blue Hill Managed Services site.	No exceptions noted.
CC2.3.2	The entity's security and availability commitments and the associated system requirements are documented in customer contracts.	Inspected customer contracts for a sample of current customers to determine that the entity's security and availability commitments and the associated system requirements were documented in customer contracts for each customer sampled.	No exceptions noted.
CC2.3.3	A phone hotline and service desk e-mail address are available to external users to report security or availability failures, incidents, concerns, and other complaints to BHDS personnel.	Inspected the incident response policy and company website to determine that a phone hotline and service desk e-mail address was available to external users to report security or availability failures, incidents, concerns, and other complaints to BHDS personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	Account management personnel conduct meetings with client personnel on a client specified basis to review and discuss compliance with SOWs.	Inquired of the director of strategic services regarding SOW compliance to determine that account management personnel conducted meetings with client personnel on a client specified basis to review and discuss compliance with SOWs.	No exceptions noted.
		Inspected the recurring meeting invite for a sample of current clients to determine that meetings were conducted on a client specified basis during the review period for each client sampled.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.
CC3.1.2	Management holds a strategy meeting on at least an annual basis that discusses and aligns internal control responsibilities, performance measures, and incentives with company business objectives.	Inspected the meeting invite, attendees, and meeting minutes from the strategy meeting to determine that management held a strategy meeting that discussed and aligned internal control responsibilities, performance measures, and incentives with company business objectives during the review period.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	Documented policies and procedures are in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in identifying business objective risks, assessing changes to the system, and developing risk management strategies as a part of the risk assessment process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.2	Security stakeholders perform a risk assessment on an annual basis that identifies and analyzes the business and security risks. Risks identified are formally documented, along with mitigation strategies, and reviewed by management.	Inspected the most recently completed risk assessment to determine that security stakeholders performed a risk assessment that identified and analyzed the business and security risks and risks identified were formally documented, along with mitigation strategies, and reviewed by management during the review period.	No exceptions noted.
CC3.2.3	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC3.2.4	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A documented policy and procedure is in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	Inspected the fraud assessment policy and procedures to determine that a documented policy and procedure was in place to guide personnel in identifying the potential for fraud as part of the risk assessment process.	No exceptions noted.
CC3.3.2	Security stakeholders perform a risk assessment on an annual basis that considers the potential for fraud in assessing risks to the achievement of objectives.	Inspected the most recently completed risk assessment to determine that security stakeholder performed a risk assessment that considered the potential for fraud in assessing risks to the achievement of objectives during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the director of strategic services regarding third-party security updates to determine that the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected an example security update e-mail from a third-party to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
CC3.4.2	Security stakeholders perform a risk assessment on an annual basis that considers the impact of changes to the system. Risks that are identified are rated using a risk evaluation process and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment to determine that security stakeholders performed a risk assessment that considered the impact of changes to the system and that risks that were identified were rated using a risk evaluation process and were formally documented, along with mitigation strategies, for management review during the review period.	No exceptions noted.
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC4.1.2	Enterprise monitoring applications are utilized to monitor processing activities for exceptions and anomalies.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor processing activities for exceptions and anomalies.	No exceptions noted.
CC4.1.3	Enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor operational performance of production servers and network devices.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded, or controlled events are triggered.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded, or controlled events were triggered.	No exceptions noted.
CC4.1.5	An IDS is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	Inspected the IDS ruleset, alerting configurations, and an example alert generated during the review period to determine that an IDS was utilized to detect, analyze, and manage the network security perimeter and was configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	No exceptions noted.
CC4.1.6	The supervisor of enterprise operations reviews shifts logs on a weekly basis to help ensure response to processing exceptions occurs.	Inspected evidence of shift log reviews for a sample of weeks during the review period to determine that the supervisor of enterprise operations reviewed shifts logs to help ensure response to processing exceptions occurred for each week sampled.	No exceptions noted.
CC4.1.7	The supervisor of enterprise operations reviews incident status reports on a weekly basis to monitor the status of service requests and incidents.	Inquired of the director of strategic services regarding the review of incident status reports to determine that the supervisor of enterprise operations reviewed incident status reports on a weekly basis to monitor the status of service requests and incidents.	No exceptions noted.
		Inspected the incident status report review for a sample of weeks during the review period to determine that the supervisor of enterprise operations reviewed incident status reports for each week sampled.	No exceptions noted.
CC4.1.8	Managers are actively involved in supervising and reviewing the work of subordinate employees and are responsible for helping to ensure compliance to client and company operating procedures.	Inquired of the director of office administration regarding manager practices to determine that managers were actively involved in supervising and reviewing the work of subordinate employees and were responsible for helping to ensure compliance to client and company operating procedures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the business process procedures to determine that managers were actively involved in supervising and reviewing the work of subordinate employees.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities.	Inspected the incident response procedures to determine that documented incident response procedures were in place to guide personnel in server and network outage response, escalation, and resolution activities.	No exceptions noted.
CC4.2.2	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.
CC4.2.3	The entity's IT security group monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by senior management.	Inquired of the director of strategic services regarding third-party security updates to determine that the impact of changes to applicable laws or regulations were considered by senior management.	No exceptions noted.
		Inspected an example security update e-mail from a third-party to determine that the entity's IT security group monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
CC4.2.4	The supervisor of enterprise operations reviews incident status reports on a weekly basis to monitor the status of service requests and incidents.	Inquired of the director of strategic services regarding the review of incident status reports to determine that the supervisor of enterprise operations reviewed incident status reports on a weekly basis to monitor the status of service requests and incidents.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the incident status report review for a sample of weeks during the review period to determine that the supervisor of enterprise operations reviewed incident status reports for each week sampled.	No exceptions noted.
CC4.2.5	An executive management team comprised of security personnel has been established to guide the company in managing security and availability risks.	Inquired of the director of strategic services regarding the executive management team to determine that a group comprised of security personnel was established to guide the company in managing security and availability risks.	No exceptions noted.
		Inspected the organizational chart to determine that an executive management team was comprised of security personnel.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	Documented policies and procedures are in place to guide personnel in selecting and developing control activities that contribute to the mitigation of risks when performing the risk assessment process.	Inspected the risk assessment methodology to determine that documented policies and procedures were in place to guide personnel in selecting and developing control activities that contributed to the mitigation of risks when performing the risk assessment process.	No exceptions noted.
CC5.1.2	Security stakeholders perform a formal risk assessment on an annual basis that includes an analysis of risk mitigation control activities and considers how the environment, complexity, nature, and scope of its operations affect the selection and development of control activities.	Inspected the most recently completed risk assessment to determine that security stakeholders performed a risk assessment that included an analysis of risk mitigation control activities and considered how the environment, complexity, nature, and scope of its operations affected the selection and development of control activities during the review period.	No exceptions noted.
CC5.1.3	Risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recently completed risk assessment to determine that risk owners selected and developed control activities to mitigate the risks identified during the risk assessment process and that control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Risk owners select and develop control activities over technology to support the achievement of objectives as an output from the annual risk assessment process. The control activities are documented within the mitigation plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recently completed risk assessment to determine that risk owners selected and developed control activities over technology to support the achievement of objectives as an output from the risk assessment process and that control activities were documented within the mitigation plans that were created by the risk owners for risks above the tolerable threshold during the review period.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Information security policies and procedures are in place to guide personnel in the entity's security practices and are communicated to personnel via the company intranet.	Inspected the security policies on the company intranet to determine that information security policies and procedures were in place to guide personnel in the entity's security practices and were communicated to personnel via the company intranet.	No exceptions noted.
CC5.3.2	New employees and contractors are required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Inspected the signed confidentiality agreements for a sample of employees and contractors hired during the review period to determine that new employees and contractors were required to sign a confidentiality agreement upon hire agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties for each employee and contractor sampled.	No exceptions noted.
CC5.3.3	Documented operating policies and procedures are in place that define information system baseline requirements, establish, and monitor alarm levels, and select measures, analytic techniques, and tools to be used in managing system security and availability.	Inspected the operating policies and procedures to determine that documented operating policies and procedures were in place that defined information system baseline requirements, established, and monitored alarm levels, and selected measures, analytic techniques, and tools to be used in managing system security and availability.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.4	An employee sanction procedure is in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	Inspected the employee handbook procedures to determine that an employee sanction procedure was in place and documented within the employee handbook communicating that an employee may be terminated for noncompliance with a policy or procedure.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	A formally documented system hardening procedure for installation and maintenance of production servers is in place that includes the requirement for access control systems to enforce logical access.	Inspected the system hardening procedures to determine that a formally documented system hardening procedure for installation and maintenance of production servers was in place that included the requirement for access control systems to enforce logical access.	No exceptions noted.
CC6.1.2	Access to managed infrastructure is secured via an encrypted VPN that requires two-factor authentication using RSA SecurID technology that includes the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	Observed the VPN authentication process to determine that access to managed infrastructure required two-factor authentication using RSA SecurID technology that included the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	No exceptions noted.
		Inspected the VPN and RSA system configurations to determine that access to managed infrastructure was secured via an encrypted VPN that required two-factor authentication using RSA SecurID technology.	No exceptions noted.
CC6.1.3	The managed infrastructure is configured to enforce the following user account and password controls: <ul style="list-style-type: none"> • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history • Invalid password account lockout threshold 	Inspected the managed infrastructure authentication configurations to determine that the managed infrastructure was configured to enforce the following user account and password controls: <ul style="list-style-type: none"> • Password minimum length • Password expiration intervals • Password complexity requirements • Password minimum history • Invalid password account lockout threshold 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.4	Remote access to managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with remote access to managed environments with the assistance of the director of strategic services to determine that remote access to managed environments was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.5	Administrator access within the client firewall systems is restricted to user accounts accessible by authorized personnel.	Inspected the firewall system administrator account listings for a sample of client firewall systems with the assistance of the director of strategic services to determine that administrator access within the client firewall systems was restricted to user accounts accessible by authorized personnel for each firewall system sampled.	No exceptions noted.
CC6.1.6	Administrator access within the client VPN systems is restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrator account listings for a sample of client VPN systems with the assistance of the director of strategic services to determine that administrator access within client VPN systems was restricted to user accounts accessible by authorized personnel for each client VPN system sampled.	No exceptions noted.
CC6.1.7	Administrator access within the BHDS firewall system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS firewall system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.8	Administrator access within the BHDS VPN system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS VPN system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS VPN system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.1.9	Administrator access within the managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the user access permissions for a sample of client systems with the assistance of the director of strategic services to determine that administrator access within the managed environment was restricted to user accounts accessible by authorized personnel for each client system sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	A hiring manager completes a new hire setup form and submits it via a service desk ticket to IT for the creation or modification of user accounts.	Inspected the new employee user set up form and the resulting service desk ticket for a sample of employees hired during the review period to determine that a hiring manager completed a new hire setup form and submitted it via a service desk ticket to IT for the creation or modification of user accounts for each employee sampled.	No exceptions noted.
CC6.2.2	Operations personnel require authorization from an authorized client representative for the modification of client user account access privileges.	Inquired of the director of strategic services regarding authorization for the modification of client user account access privileges to determine that operations personnel required authorization from an authorized client representative for the modification of client user account access privileges.	No exceptions noted.
		Inspected evidence of authorization for a sample of client user account access privilege modification requests during the review period to determine that authorization from a client representative was obtained for each request sampled.	No exceptions noted.
CC6.2.3	A termination checklist is utilized to help ensure that specific components of the termination process are consistently executed.	Inspected the termination checklist for a sample of employees terminated during the review period to determine that a termination checklist was utilized to help ensure that specific components of the termination process were consistently executed for each terminated employee sampled.	No exceptions noted.
CC6.2.4	Terminated employees' system access rights to client systems are revoked as a component of the termination process.	Inspected the client system user access privileges for a sample of client systems and employees terminated during the review period to determine that access privileges to client systems were revoked for each client system and terminated employee sampled as a component of the termination process.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.2.5	IT personnel perform logical user access reviews on a quarterly basis to help ensure that access is properly restricted.	Inspected the quarterly access review ticket for a sample of quarters during the review period to determine that IT personnel performed logical access reviews to help ensure that access was properly restricted for each quarter sampled.	No exceptions noted.
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	A hiring manager completes a new hire setup form and submits it via a service desk ticket to IT for the creation or modification of user accounts.	Inspected the new employee user set up form and the resulting service desk ticket for a sample of employees hired during the review period to determine that a hiring manager completed a new hire setup form and submitted it via a service desk ticket to IT for the creation or modification of user accounts for each employee sampled.	No exceptions noted.
CC6.3.2	Operations personnel require authorization from an authorized client representative for the modification of client user account access privileges.	Inquired of the director of strategic services regarding authorization for the modification of client user account access privileges to determine that operations personnel required authorization from an authorized client representative for the modification of client user account access privileges.	No exceptions noted.
		Inspected evidence of authorization for a sample of client user account access privilege modification requests during the review period to determine that authorization from a client representative was obtained for each request sampled.	No exceptions noted.
CC6.3.3	A termination checklist is utilized to help ensure that specific components of the termination process are consistently executed.	Inspected the termination checklist for a sample of employees terminated during the review period to determine that a termination checklist was utilized to help ensure that specific components of the termination process were consistently executed for each terminated employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.4	Terminated employees' system access rights to client systems are revoked as a component of the termination process.	Inspected the client system user access privileges for a sample of client systems and employees terminated during the review period to determine that access privileges to client systems were revoked for each client system and terminated employee sampled as a component of the termination process.	No exceptions noted.
CC6.3.5	Administrator access within the client firewall systems is restricted to user accounts accessible by authorized personnel.	Inspected the firewall system administrator account listings for a sample of client firewall systems with the assistance of the director of strategic services to determine that administrator access within the client firewall systems was restricted to user accounts accessible by authorized personnel for each firewall system sampled.	No exceptions noted.
CC6.3.6	Administrator access within the client VPN systems is restricted to user accounts accessible by authorized personnel.	Inspected the VPN system administrator account listings for a sample of client VPN systems with the assistance of the director of strategic services to determine that administrator access within client VPN systems was restricted to user accounts accessible by authorized personnel for each client VPN system sampled.	No exceptions noted.
CC6.3.7	Administrator access within the BHDS firewall system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS firewall system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS firewall system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.8	Administrator access within the BHDS VPN system is restricted to user accounts accessible by authorized personnel.	Inspected the BHDS VPN system administrator account listing with the assistance of the director of strategic services to determine that administrator access within the BHDS VPN system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.3.9	Administrator access within the managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the user access permissions for a sample of client systems with the assistance of the director of strategic services to determine that administrator access within the managed environment was restricted to user accounts accessible by authorized personnel for each client system sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.10	IT personnel perform logical user access reviews on a quarterly basis to help ensure that access is properly restricted.	Inspected the quarterly access review ticket for a sample of quarters during the review period to determine that IT personnel performed logical access reviews to help ensure that access was properly restricted for each quarter sampled.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	Hiring managers provide authorization prior to physical access privileges being granted to new employees.	Inquired of the director of office administration regarding physical access restrictions to determine that hiring managers provided authorization prior to physical access privileges being granted to new employees.	No exceptions noted.
		Inspected evidence of authorization for a sample of employees hired during the review period to determine that hiring managers provided authorization to grant physical access privileges for each employee sampled.	No exceptions noted.
CC6.4.2	Badge access privileges assigned to terminated employees are revoked as a component of the employee termination process.	Inquired of the chief facilities engineer regarding the termination process to determine that badge access privileges assigned to terminated employees were revoked as a component of the employee termination process.	No exceptions noted.
		Inspected the badge access listing for a sample of employees terminated during the review period to determine that badge access privileges were revoked for each terminated employee sampled.	No exceptions noted.
CC6.4.3	An account manager reviews badge access privileges on a monthly basis to help ensure that badge access privileges are authorized.	Inquired of an account manager regarding the review of badge access privileges to determine that an account manager reviewed badge access privileges on a monthly basis to help ensure that badge access privileges were authorized.	No exceptions noted.
		Inspected the badge access privileges review documentation for a sample of months during the review period to determine that an account manager reviewed badge access privileges for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.4	Administrator access within the badge access system is restricted to user accounts accessible by authorized personnel.	Inspected the badge access system administrator account listing with the assistance of the chief facilities engineer to determine that administrator access within the badge access system was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC6.4.5	The badge access system logs access attempts that are traceable to specific badge access cards. Facilities and building engineering personnel review badge access system logs on an ad-hoc basis.	Inquired of the chief facilities engineer regarding the badge access system to determine that facilities and building engineering personnel reviewed badge access system logs on an ad-hoc basis.	No exceptions noted.
		Inspected an example badge access system log generated during the review period to determine that the badge access system logged access attempts that were traceable to specific badge access cards.	No exceptions noted.
CC6.4.6	Production infrastructure is housed within a secure data center.	Observed the production infrastructure located within the data center to determine that production infrastructure was housed within a secure data center.	No exceptions noted.
CC6.4.7	Production infrastructure is secured in locked cabinets within the data center.	Observed the production infrastructure to determine that production infrastructure was secured in locked cabinets within the data center.	No exceptions noted.
CC6.4.8	A badge access system is utilized to control access to the data center.	Observed the badge access system to determine that a badge access system was utilized to control access to the data center.	No exceptions noted.
		Inspected the badge access listing and zone definitions to determine that a badge access system was utilized to control access to the data center.	No exceptions noted.
CC6.4.9	Visitors are required to be escorted when accessing the data center.	Observed the visitor access process to determine that visitors were required to be escorted when accessing the data center.	No exceptions noted.
CC6.4.10	Visitors are required to sign a visitor log upon entering the data center.	Observed the visitor entrance process to determine that visitors were required to sign a visitor log upon entering the data center.	No exceptions noted.
		Inspected the data center visitor logs for a sample of months during the review period to determine that visitor logs were in place for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.4.11	A digital surveillance system is in place to monitor and record activity at the entrance to and throughout the data center.	Observed the digital surveillance cameras throughout the data center to determine that a digital surveillance system was in place to monitor and record activity at the entrance to and throughout the data center.	No exceptions noted.
		Inspected an example historical image recorded during the review period to determine that a digital surveillance system was in place to monitor the data center.	No exceptions noted.
CC6.4.12	Recordings from the digital surveillance cameras are retained for a minimum of three months.	Inspected an example historical image recorded during the review period to determine that recordings from the digital surveillance cameras were retained for a minimum of three months.	No exceptions noted.
CC6.4.13	Access to the data center is restricted to badge access cards assigned to authorized personnel.	Inspected the data center access listing with the assistance of the director of strategic services to determine that access to the data center was restricted to badge access cards assigned to authorized personnel.	No exceptions noted.
CC6.4.14	Data center walls extend from the real floor to the real ceiling restricting physical access to the data center.	Observed the data center walls to determine that data center walls extended from the real floor to the real ceiling restricting physical access to the data center.	No exceptions noted.
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	Inspected the third-party media storage agreement to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	No exceptions noted.
		Inspected the third-party media storage invoices for a sample of months during the review period to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media for each month sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.5.2	Property pass forms are utilized to document the removal of equipment from the data center. Property pass forms are required to be approved by personnel holding one of the following positions: <ul style="list-style-type: none">• Chief facilities engineer• Account manager• Director strategic services	Inquired of the chief facilities engineer regarding property pass forms to determine that property pass forms were utilized to document the removal of equipment from the data center and that property pass forms were required to be approved by personnel holding one of the following positions: <ul style="list-style-type: none">• Chief facilities engineer• Account manager• Director strategic services	No exceptions noted.
		Inspected evidence of approval for a sample of property pass forms documented during the review period to determine that each equipment removal sampled was approved by personnel holding one of the following positions: <ul style="list-style-type: none">• Chief facilities engineer• Account manager• Director strategic services	No exceptions noted.
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Firewall systems are in place to filter unauthorized inbound network traffic from the internet.	Inspected the firewall system configurations for a sample of firewall systems to determine that firewall systems were in place to filter unauthorized inbound network traffic from the internet for each firewall sampled.	No exceptions noted.
CC6.6.2	The firewall systems are configured to deny any type of network connection that is not explicitly authorized by a firewall rule.	Inspected the firewall system configurations for a sample of firewall systems to determine that the firewall systems were configured to deny any type of network connection that was not explicitly authorized by a firewall rule for each firewall sampled.	No exceptions noted.
CC6.6.3	An IDS is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	Inspected the IDS ruleset, alerting configurations, and an example alert generated during the review period to determine that an IDS was utilized to detect, analyze, and manage the network security perimeter and was configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.4	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC6.6.5	Encrypted VPNs are utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	Inquired of a senior network engineer regarding remote network access to client environments to determine that encrypted VPNs were utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	No exceptions noted.
		Inspected the VPN authentication and encryption configurations for a sample of VPN systems to determine that encrypted VPNs were utilized for remote network access to client environments for each VPN system sampled.	No exceptions noted.
CC6.6.6	Access to managed infrastructure is secured via an encrypted VPN that requires two-factor authentication using RSA SecurID technology that includes the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	Observed the VPN authentication process to determine that access to managed infrastructure required two-factor authentication using RSA SecurID technology that included the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	No exceptions noted.
		Inspected the VPN and RSA system configurations to determine that access to managed infrastructure was secured via an encrypted VPN that required two-factor authentication using RSA SecurID technology.	No exceptions noted.
CC6.6.7	Remote access to managed environments is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with remote access to managed environments with the assistance of the director of strategic services to determine that remote access to managed environments was restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	Encrypted VPNs are utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	Inquired of a senior network engineer regarding remote network access to client environments to determine that encrypted VPNs were utilized for remote network access to client environments to help ensure the privacy and integrity of data passing over the public network.	No exceptions noted.
		Inspected the VPN authentication and encryption configurations for a sample of VPN systems to determine that encrypted VPNs were utilized for remote network access to client environments for each VPN system sampled.	No exceptions noted.
CC6.7.2	Access to managed infrastructure is secured via an encrypted VPN that requires two-factor authentication using RSA SecurID technology that includes the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	Observed the VPN authentication process to determine that access to managed infrastructure required two-factor authentication using RSA SecurID technology that included the following: <ul style="list-style-type: none"> • User account • PIN • Individual token generator 	No exceptions noted.
		Inspected the VPN and RSA system configurations to determine that access to managed infrastructure was secured via an encrypted VPN that required two-factor authentication using RSA SecurID technology.	No exceptions noted.
CC6.7.3	Open system environments run on dedicated and physically separate processing environments.	Inspected the physical system inventories for a sample of open system clients to determine that open system environments ran on dedicated and physically separate processing environments for each client sampled.	No exceptions noted.
CC6.7.4	Open system environments utilizing shared SAN disk storage are segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments.	Inspected the SAN disk configurations for a sample of open system clients utilizing shared SAN disk storage to determine that open system environments utilizing SAN disk storage were segregated via fiber switch SAN zoning and storage array logical unit number level masking assignments for each client sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	<p>The antivirus solution is configured to protect registered production servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> • Scan for updates to antivirus definitions and update registered clients on a continuous basis • Scan registered clients on a continuous basis 	<p>Inspected the antivirus scan configurations to determine that the antivirus solution was configured to protect registered production servers and workstations with the following configurations:</p> <ul style="list-style-type: none"> • Scan for updates to antivirus definitions and update registered clients on a continuous basis • Scan registered clients on a continuous basis 	No exceptions noted.
CC6.8.2	The ability to implement server upgrades within the client managed environments is restricted to user accounts accessible to authorized personnel.	Inspected the user access permissions for a sample of client systems with the assistance of the director of strategic services to determine that the ability to implement server upgrades within the managed environments was restricted to user accounts accessible by authorized personnel for each client environment sampled.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC7.1.2	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.3	An IDS is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	Inspected the IDS ruleset, alerting configurations, and an example alert generated during the review period to determine that an IDS was utilized to detect, analyze, and manage the network security perimeter and was configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	No exceptions noted.
CC7.1.4	The firewall systems are configured to log unauthorized remote access attempts to the BHDS environment and client environments. The senior director of network services and senior network engineers review firewall system logs on an ad hoc basis.	Inquired of the senior network engineer regarding the firewall systems to determine that the senior director of network services and senior network engineers reviewed firewall system logs on an ad hoc basis.	No exceptions noted.
		Inspected the firewall system logging configurations and example firewall system logs generated during the review period for a sample of firewall systems to determine that the firewall systems were configured to log unauthorized remote access attempts to the BHDS environment and client environments for each firewall system sampled.	No exceptions noted.
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Enterprise monitoring applications are utilized to monitor processing activities for exceptions and anomalies.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor processing activities for exceptions and anomalies.	No exceptions noted.
CC7.2.2	Enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor operational performance of production servers and network devices.	No exceptions noted.
CC7.2.3	Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure.	Inquired of the director of strategic services regarding data center and client infrastructure monitoring to determine that operations personnel were available on a 24 hour per day basis to monitor data center and client infrastructure.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available on a 24 hour per day basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.4	Service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.	Inspected the staffing schedule for a sample of months during the review period to determine that service desk personnel were available on a 24 hour per day basis to monitor client environments and respond to support requests for each month sampled.	No exceptions noted.
CC7.2.5	A maintenance and service agreement is in place with an ISP to provide coverage for communications components on a 24 hour per day basis.	Inquired of the director of strategic services regarding the ISP to determine that a maintenance and service agreement was in place with an ISP to provide coverage for communications components on a 24 hour per day basis.	No exceptions noted.
		Inspected the maintenance and service agreement for the ISP to determine that a maintenance and service agreement was in place with an ISP to provide coverage for communications components.	No exceptions noted.
CC7.2.6	An IDS is utilized to detect, analyze, and manage the network security perimeter and is configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	Inspected the IDS ruleset, alerting configurations, and an example alert generated during the review period to determine that an IDS was utilized to detect, analyze, and manage the network security perimeter and was configured to send e-mail alert notifications to network personnel for possible or actual security breaches.	No exceptions noted.
CC7.2.7	Third-party external vulnerability scans of the production network are performed on a monthly basis and results are sent to the network engineering team.	Inspected the vulnerability scan reports for a sample of months during the review period to determine that third-party external vulnerability scans of the production network were performed, and results were sent to the network engineering team for each month sampled.	No exceptions noted.
CC7.2.8	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	Incident response procedures are in place that outline the response procedures to security events and includes lessons learned to evaluate the effectiveness of the procedures.	Inspected the incident response procedures to determine that incident response procedures were in place that outlined the response procedures to security events and included lessons learned to evaluate the effectiveness of the procedures.	No exceptions noted.
CC7.3.2	Documented computer operations procedures are in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	Inspected the computer operations procedures to determine that documented computer operations procedures were in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	No exceptions noted.
CC7.3.3	An automated ticketing system is utilized to prioritize, log, and track resolution steps for service requests and incidents.	Inspected the incident tickets for a sample of service requests and incidents logged during the review period to determine that an automated ticketing system was utilized to prioritize, log, and track resolution steps for service requests and incidents for each service request and incident sampled.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	Documented incident response procedures are in place and include the following to guide personnel throughout the incident response process: <ul style="list-style-type: none"> • Point of contacts • Incident notification • Incident communication • Incident resolution • Escalation and communication to affected parties 	Inspected the incident response procedures to determine that documented incident response procedures were in place and included the following to guide personnel throughout the incident response process: <ul style="list-style-type: none"> • Point of contacts • Incident notification • Incident communication • Incident resolution • Escalation and communication to affected parties 	No exceptions noted.
CC7.4.2	Documented computer operations procedures are in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	Inspected the computer operations procedures to determine that documented computer operations procedures were in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	An automated ticketing system is utilized to prioritize, log, and track resolution steps for service requests and incidents.	Inspected the incident tickets for a sample of service requests and incidents logged during the review period to determine that an automated ticketing system was utilized to prioritize, log, and track resolution steps for service requests and incidents for each service request and incident sampled.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Incident response procedures are in place that outline the response procedures to security events and includes lessons learned to evaluate the effectiveness of the procedures.	Inspected the incident response procedures to determine that incident response procedures were in place that outlined the response procedures to security events and included lessons learned to evaluate the effectiveness of the procedures.	No exceptions noted.
CC7.5.2	Documented computer operations procedures are in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	Inspected the computer operations procedures to determine that documented computer operations procedures were in place to guide personnel in prioritizing, logging, and tracking service requests and incidents through resolution and notifying affected parties.	No exceptions noted.
CC7.5.3	An automated ticketing system is utilized to prioritize, log, and track resolution steps for service requests and incidents.	Inspected the incident tickets for a sample of service requests and incidents logged during the review period to determine that an automated ticketing system was utilized to prioritize, log, and track resolution steps for service requests and incidents for each service request and incident sampled.	No exceptions noted.
CC7.5.4	Security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	Inquired of the director of strategic services regarding vulnerability scan remediation to determine that security operations and infrastructure teams track, review, and remediate security vulnerabilities identified in the infrastructure vulnerability scans according to security remediation standards.	No exceptions noted.
		Inspected the most recent vulnerability scan communication to determine that security operations and infrastructure teams track, review, and remediate infrastructure vulnerability scans.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Documented procedures are in place to help guide the BHDS and client change management processes.	Inspected the change management procedures to determine that documented procedures were in place to help guide the BHDS and client change management processes.	No exceptions noted.
CC8.1.2	BHDS management and engineers are notified of changes and ongoing and upcoming projects that affect the system via monthly change management meetings.	Inquired of the director of strategic services regarding change management meetings to determine that BHDS management and engineers were notified of changes and ongoing and upcoming projects that affected the system via monthly change management meetings.	No exceptions noted.
		Inspected the recurring change management calendar invite to determine that BHDS management and engineers were notified of changes and ongoing and upcoming projects that affected the system via the monthly change management meetings.	No exceptions noted.
CC8.1.3	A service desk ticketing system is utilized to centrally maintain client change requests and processing routine exceptions.	Inspected the service desk tickets for a sample of client changes and processing exceptions generated during the review period to determine that a service desk ticketing system was utilized to centrally maintain client change requests and processing routine exceptions for each client change and processing exception sampled.	No exceptions noted.
CC8.1.4	A service desk ticketing system is in place to centrally maintain, manage, and monitor upgrade and maintenance activities.	Inspected change tickets for a sample of upgrade and maintenance activities during the review period to determine that a service desk ticketing system was in place to centrally maintain, manage, and monitor each upgrade and maintenance activity sampled.	No exceptions noted.
CC8.1.5	Operations management requires client personnel to perform UAT for upgrades prior to implementation.	Inquired of the director of strategic services regarding upgrades to determine that operations management required client personnel to perform UAT for upgrades prior to implementation.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of UAT for a sample of upgrades implemented during the review period to determine that client personnel performed UAT for each upgrade sampled.	No exceptions noted.
CC8.1.6	Operations management requires client personnel to approve upgrades prior to implementation.	Inquired of the director of strategic services regarding upgrades to determine that operations management required client personnel to approve upgrades prior to implementation.	No exceptions noted.
		Inspected evidence of approval for a sample of upgrades implemented during the review period to determine that client personnel approved each upgrade sampled.	No exceptions noted.
CC8.1.7	The ability to implement server upgrades within the client managed environments is restricted to user accounts accessible to authorized personnel.	Inspected the user access permissions for a sample of client systems with the assistance of the director of strategic services to determine that the ability to implement server upgrades within the managed environments was restricted to user accounts accessible by authorized personnel for each client environment sampled.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Documented policies and procedures are in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as a part of the risk assessment process.	Inspected the risk assessment methodology to determine that policies and procedures were in place to guide personnel in identifying, selecting, and developing risk management strategies specifically addressing the risks arising from potential business disruptions as a part of the risk assessment process.	No exceptions noted.
CC9.1.2	Security stakeholders perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions.	Inspected the most recently completed risk assessment to determine that security stakeholders performed a risk assessment that included an evaluation of risk mitigation control activities for risks arising from potential business disruptions during the review period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1.3	BHDS utilizes a cyber reliability insurance policy that would allow for continued support to return to successful business operations if an impactful cybersecurity disruption occurred.	Inspected the certificate of liability insurance to determine that BHDS utilized a cyber reliability insurance policy that allowed for continued support to return to successful business operations if an impactful cybersecurity disruption occurred.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	<p>A vendor management policy is in place that address the following:</p> <ul style="list-style-type: none"> • Specific requirements for a vendor and business partner • Due diligence process prior to accepting new vendors or business partners • Contract considerations • Monitoring of vendors 	<p>Inspected the vendor management policy to determine that a vendor management policy was in place that addressed the following:</p> <ul style="list-style-type: none"> • Specific requirements for a vendor and business partner • Due diligence process prior to accepting new vendors or business partners • Contract considerations • Monitoring of vendors 	No exceptions noted.
CC9.2.2	Security stakeholders perform a risk assessment on an annual basis whereby vendor risks are considered and include mitigation control activities for risks arising from vendor risks.	Inspected the most recently completed risk assessment to determine that security stakeholders performed a risk assessment whereby vendor risks were considered and included mitigation control activities for risks arising from vendor risks during the review period.	No exceptions noted.

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Documented incident response procedures are in place to guide personnel in server and network outage response, escalation, and resolution activities.	Inspected the incident response procedures to determine that documented incident response procedures were in place to guide personnel in server and network outage response, escalation, and resolution activities.	No exceptions noted.
A1.1.2	Enterprise monitoring applications are utilized to monitor operational performance of production servers and network devices.	Inspected the enterprise monitoring configurations to determine that enterprise monitoring applications were utilized to monitor operational performance of production servers and network devices.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1.3	Enterprise monitoring applications are configured to send e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored systems.	Inspected the alerting configurations from the enterprise monitoring applications and example e-mail alert notifications generated during the review period to determine that the enterprise monitoring applications were configured to send e-mail alert notifications to operations personnel when predefined thresholds were exceeded on monitored systems.	No exceptions noted.
A1.1.4	Operations personnel are available on a 24 hour per day basis to monitor data center and client infrastructure.	Inquired of the director of strategic services regarding data center and client infrastructure monitoring to determine that operations personnel were available on a 24 hour per day basis to monitor data center and client infrastructure.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available on a 24 hour per day basis.	No exceptions noted.
A1.1.5	Service desk personnel are available on a 24 hour per day basis to monitor client environments and respond to support requests.	Inspected the staffing schedule for a sample of months during the review period to determine that service desk personnel were available on a 24 hour per day basis to monitor client environments and respond to support requests for each month sampled.	No exceptions noted.
A1.1.6	The senior director of enterprise operations reviews operational statistics and trends on a weekly basis that may affect the availability of systems.	Inspected the process activity review for a sample of weeks during the review period to determine that the senior director of enterprise operations reviewed operational statistics and trends that may have affected the availability of systems for each week sampled.	No exceptions noted.
A1.1.7	Load balancing and replication devices are in place to distribute requests and provide failover services in the event of system failures.	Inspected the load balancing and replication device configurations to determine that load balancing and replication devices were in place to distribute requests and provide failover services in the event of system failures.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	Documented SLAs that define backup and recovery services for clients are in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions.	Inspected the SLAs for a sample of current clients subscribed to disaster recovery services to determine that documented SLAs that defined backup and recovery services were in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions for each client sampled.	No exceptions noted.
A1.2.2	Multiple backup systems are utilized to perform backups of client data according to specifications documented in the SLA.	Inspected the backup system configurations and example backup logs generated during the review period for a sample of current clients subscribed to data backup services to determine that multiple backup systems were utilized to perform backups of client data according to specifications documented in the SLA for each client sampled.	No exceptions noted.
A1.2.3	Operations personnel monitor the status of backup processing on a 24 hour per day basis. Processing errors are reported to technical personnel for resolution and documented in a service desk ticket.	Inquired of the director of strategic services regarding backup monitoring to determine that operations personnel monitored the status of backup processing on a 24 hour per day basis.	No exceptions noted.
		Inspected the staffing schedule to determine that operations personnel were available to monitor the status of backup processing on a 24 hour per day basis.	No exceptions noted.
		Inspected the service desk tickets for a sample of processing errors generated during the review period to determine that processing errors were reported to technical personnel for resolution and documented in a service desk ticket for each processing error sampled.	No exceptions noted.
A1.2.4	<p>The data center is equipped with the following environmental protection equipment with third-party inspections occurring at least annually:</p> <ul style="list-style-type: none"> • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units 	<p>Observed the environmental protection equipment within the data center to determine that the data center was equipped with the following environmental protection equipment:</p> <ul style="list-style-type: none"> • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units 	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		<p>Inspected the most recent environmental protection equipment inspection reports to determine that the following environmental protection equipment was inspected by a third party during the review period:</p> <ul style="list-style-type: none"> • Fire detection and suppression equipment • UPS systems • Generators • Air conditioning units 	No exceptions noted.
A1.2.5	A third-party media storage provider is utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	Inspected the third-party media storage agreement to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media.	No exceptions noted.
		Inspected the third-party media storage invoices for a sample of months during the review period to determine that a third-party media storage provider was utilized for secure off-site storage of backup media and the disposal and destruction of expired media for each month sampled.	No exceptions noted.
A1.2.6	Operations personnel rotate backup media to the off-site third-party media vaulting company on a daily, weekly, and monthly basis in accordance with client specifications.	Inspected the tape transfer manifests for a sample of current clients subscribed to managed backup and tape rotation services and dates, weeks, and months during the review period to determine that operations personnel rotated backup media to the off-site third-party media vaulting company in accordance with client specifications for each client, date, week, and month sampled.	No exceptions noted.
A1.2.7	Operations personnel maintain backup and recovery procedures for clients subscribed to hot-site services and are tested according to client requirements.	Inspected the backup and recovery procedures for a sample of current clients subscribed to hot-site services to determine that operations personnel-maintained backup and recovery procedures for each client sampled.	No exceptions noted.
		Inspected the most recent backup and recovery test results for a sample of current clients subscribed to hot-site services to determine that backup and recovery procedures were tested during the review period for each client sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Documented SLAs that define backup and recovery services for clients are in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions.	Inspected the SLAs for a sample of current clients subscribed to disaster recovery services to determine that documented SLAs that defined backup and recovery services were in place to guide personnel in performing backup and recovery procedures in accordance with SLA provisions for each client sampled.	No exceptions noted.
A1.3.2	Operations personnel maintain backup and recovery procedures for clients subscribed to hot-site services and are tested according to client requirements.	Inspected the backup and recovery procedures for a sample of current clients subscribed to hot-site services to determine that operations personnel-maintained backup and recovery procedures for each client sampled.	No exceptions noted.
		Inspected the most recent backup and recovery test results for a sample of current clients subscribed to hot-site services to determine that backup and recovery procedures were tested during the review period for each client sampled.	No exceptions noted.
A1.3.3	Disaster recovery plans are tested on at least an annual basis.	Inspected the disaster recovery test results to determine that disaster recovery plans were tested during the review period.	No exceptions noted.



Blue Hill Data Services | Fully Managed On-Shore Data Center Hosting Solutions

2 Blue Hill Plaza, POB 1614, Pearl River, NY 10965

Ph: 845.620.0400 | F: 845.620.1755

July 15, 2022

***Letter of Assurance: Report on Controls Placed in Operation and
Tests of Operating Effectiveness***

RE: Type 2 SOC 1 Compliance for Blue Hill Data Services

The most recent Type 2 SOC 1 examination (also known as Type 2 SSAE18) for Blue Hill Data Services was successfully completed and published in March 2022. The audit covered our controls over a 12-month period of time, from March 1, 2021 to February 28, 2022.

For the time period of March 1, 2022 to present, Blue Hill Data Services has not experienced any material changes to the internal control environment that would impact the findings as stated in the most recently published Type 2 SOC 1 report. Our next report will be published in March of 2023 covering March 1, 2022 through February 28, 2023.

Blue Hill is committed to providing our customers with the highest level of compliance in this era of enhanced corporate accountability.

If you require additional information, please contact Scott Jones at 845-875-7088 or sjones@bluehilldata.com.

Thank you for your business. We appreciate the opportunity to continue to serve your needs.

Sincerely,

John M. Lalli
Managing Director and Chief Operating Officer
Blue Hill Data Services



Blue Hill Data Services | Fully Managed On-Shore Data Center Hosting Solutions

2 Blue Hill Plaza, POB 1614, Pearl River, NY 10965

Ph: 845.620.0400 | F: 845.620.1755

July 15, 2022

***Letter of Assurance: Report on Controls Placed in Operation and
Tests of Operating Effectiveness***

RE: Type 2 SOC 2 Compliance for Blue Hill Data Services

The most recent Type 2 SOC 2 examination for Blue Hill Data Services was successfully completed and published in March 2022. The audit covered our controls over a 12-month period of time, from March 1, 2021 to February 28, 2022.

For the time period of March 1, 2022 to present, Blue Hill Data Services has not experienced any material changes to the internal control environment that would impact the findings as stated in the most recently published Type 2 SOC 2 report. Our next report will be published in March of 2023 covering March 1, 2022 through February 28, 2023.

Blue Hill is committed to providing our customers with the highest level of compliance in this era of enhanced corporate accountability.

If you require additional information, please contact Scott Jones at 845-875-7088 or sjones@bluehilldata.com.

Thank you for your business. We appreciate the opportunity to continue to serve your needs.

Sincerely,

John M. Lalli
Managing Director and Chief Operating Officer
Blue Hill Data Services

ASUS EXHIBIT F

Microsoft
Certification and
SOC Reports

Certificate of Registration

INFORMATION SECURITY MANAGEMENT SYSTEM - ISO/IEC 27001:2013

This is to certify that:

Microsoft Corporation
One Microsoft Way
Redmond
Washington
98052
USA


Holds Certificate No:

IS 755667

and operates an Information Security Management System which complies with the requirements of ISO/IEC 27001:2013 for the following scope:

The Information Security Management System (ISMS) supporting Microsoft IDEAs services including their information resources, processes and personnel inclusive of the requirements and control implementation guidance of ISO 27018:2019 for protection of personally identifiable information (PII) in public clouds acting as PII processors in accordance with the Statement of Applicability ver 3.01 dated 11/21/21.(ISO 27001:2013 Certificate IS 755667)

For and on behalf of BSI:


Carlos Pitanga, Chief Operating Officer Assurance – Americas

Original Registration Date: 2022-02-15

Latest Revision Date: 2022-02-15

Effective Date: 2022-02-15

Expiry Date: 2025-02-14

Page: 1 of 2



...making excellence a habit.™

Certificate No: **IS 755667**

Location	Registered Activities
Microsoft Corporation One Microsoft Way Redmond Washington 98052 USA	The Information Security Management System (ISMS) supporting Microsoft IDEAs services including their information resources, processes and personnel inclusive of the requirements and control implementation guidance of ISO 27018:2019 for protection of personally identifiable information (PII) in public clouds acting as PII processors



Original Registration Date: 2022-02-15
Latest Revision Date: 2022-02-15

Effective Date: 2022-02-15
Expiry Date: 2025-02-14

This certificate relates to the information security management system, and not to the products or services of the certified organization. The certificate reference number, the mark of the certification body and/or the accreditation mark may not be shown on products or stated in documents regarding products or services. Promotion material, advertisements or other documents showing or referring to this certificate, the trademark of the certification body, or the accreditation mark, must comply with the intention of the certificate. The certificate does not of itself confer immunity on the certified organization from legal obligations.

This certificate remains the property of BSI and shall be returned immediately upon request.
An electronic certificate can be authenticated [online](#). Printed copies can be validated at [www.bsigroup.com/ClientDirectory](#)
To be read in conjunction with the scope above or the attached appendix.
Information and Contact: BSI, Kitemark Court, Davy Avenue, Knowlhill, Milton Keynes MK5 8PP. Tel: + 44 345 080 9000
BSI Assurance UK Limited, registered in England under number 7805321 at 389 Chiswick High Road, London W4 4AL, UK.
A Member of the BSI Group of Companies.

Certificate of Registration

MANAGEMENT SYSTEM FOR PROTECTION OF PII IN PUBLIC CLOUDS ACTING AS
PII PROCESSORS - ISO/IEC 27018:2019

This is to certify that:

Microsoft Corporation
One Microsoft Way
Redmond
Washington
98052
USA


Holds Certificate No:

PII 755668

and operates an ISO/IEC 27001 certified ISMS that complies with the commonly accepted control objectives and controls of ISO/IEC 27018, and takes the implementation guidance of the ISO/IEC 27018 into account for the following scope:

The Information Security Management System (ISMS) supporting Microsoft IDEAs services including their information resources, processes and personnel inclusive of the requirements and control implementation guidance of ISO 27018:2019 for protection of personally identifiable information (PII) in public clouds acting as PII processors in accordance with the Statement of Applicability ver 3.01 dated 11/21/21.(ISO 27001:2013 Certificate IS 755667)

For and on behalf of BSI:


Carlos Pitanga, Chief Operating Officer Assurance – Americas

Original Registration Date: 2022-02-15

Latest Revision Date: 2022-02-15

Effective Date: 2022-02-15

Expiry Date: 2025-02-14

Page: 1 of 1



...making excellence a habit.™

Assessment Report

Microsoft Office 365

Assessment dates	02/28/2022 to 03/04/2022 (Please refer to Appendix for details)
Assessment Location(s)	Redmond (001)
Report Author	Gary Hull
Assessment Standard(s)	ISO/IEC 27001:2013, ISO 22301:2019, ISO/IEC 27017:2015, ISO/IEC 27018:2019, ISO/IEC 27701:2019



Table of contents

Executive Summary.....	4
Changes in the organization since last assessment.....	4
NCR summary graphs.....	5
Your next steps	6
NCR close out process	6
Assessment objective, scope and criteria.....	7

Statutory and regulatory requirements	7
Assessment Participants.....	8
Assessment conclusion.....	9
Findings from this assessment	9
Scope and Access Management :	9
Change Management A.12.1.2, A.14:.....	11
Vulnerability Scanning and Reporting A.12.6 Asset Management A.8:.....	14
Office 365 ISMS Management Review Clause 9.3 Context of the Organization Clause 4 :	15
ISO 27017 Controls :	17
Operations Security :	19
Human Resources Security & Supplier Management Standard A.7 - A.15:.....	20
Subscription Termination :	21
Office 365 Compliance -A.18 :	21
Cryptography - Protocols and Cyphers :	22
ISO 27701:2019 , 27018:2019 :	23
Risk Management :	26
Remediation and Exception:.....	28
SRT (Security Response) Security Response Team:.....	29
Yammer :	30
Next visit objectives, scope and criteria.....	34
Next Visit Plan	34
Appendix: Your certification structure & ongoing assessment programme.....	35
Scope of Certification	35
Assessed location(s).....	35
Certification assessment program	39
Expected outcomes for accredited certification.....	43

Definitions of findings:.....	44
How to contact BSI.....	44
Notes.....	45
Regulatory compliance.....	45

Executive Summary

- This audit certifies the processes that govern over O365 services and support features, which can be purchased in a variety of combinations by customers. For a detailed list of the services in scope please see the Office 365 Compliance Offerings paper which is updated on a regular basis with the list of services that are ISO compliant with the ISMS.
- This ISO Audit covers all worldwide locations of Microsoft O365 worldwide (excluding China). The certificates for Office 365 (all ISO/IEC 27001, 27017, 27018, 27701 and 22301) are in accordance with the requirements of the activities within the ISMS. The report is issued to the entity/client Microsoft Office 365 from the corporate headquarters of One Microsoft Way, Redmond, WA 90852
- Licenses of Microsoft O365 sold by certified partners including Microsoft affiliates and subsidiaries outside the USA, are serviced by Microsoft Corporation performing to contractual obligations. Those commitments are implemented via the ISMS that is operated by the certified entity.
- The ISO standards require an audit, which includes a requirement for vulnerability assessment and remediation of issues by the operators of the ISMS under test in this assessment.. Additionally, Microsoft has a published policy for customer performance of vulnerability assessment. Such testing can be used by Customers to further assess vulnerability risk in Office 365. Such testing can be used by Customers to further assess vulnerability risk in Office 365 under the Microsoft Cloud Penetration Testing Rules of Engagement.

Changes in the organization since last assessment

There is no significant change of the organization structure and key personnel involved in the audited management system.

No change in relation to the audited organization's activities, products or services covered by the scope of certification was identified.

There was no change to the reference or normative documents which is related to the scope of certification.

NCR summary graphs

There have been no NCRs raised.

Your next steps

NCR close out process

There were no outstanding nonconformities to review from previous assessments.

No new nonconformities were identified during the assessment. Enhanced detail relating to the overall assessment findings is contained within subsequent sections of the report.

Please refer to Assessment Conclusion and Recommendation section for the required submission and the defined timeline.

Assessment objective, scope and criteria

The objective of the assessment was to conduct a surveillance assessment and look for positive evidence to ensure that elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisation's specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan and where applicable to identify potential areas for improvement of the management system.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001, ISO 27017, ISO 27018, ISO 27701 & ISO 22301 and the defined assessment plan provided in terms of locations and areas of the system and organization to be assessed.

ISO 27001, ISO 27017, ISO 27018, ISO 27701 & ISO 22301
Microsoft 365 management system documentation

Statutory and regulatory requirements

The organization have in place a robust system to identify any Statutory, regulatory or any contractual requirements and ensure that they are monitored and met.

Assessment Participants

Name	Position	Opening Meeting	Closing Meeting	Interviewed(processes)
Patricia Anderson	PRINCIPAL PM LEAD M365 Core	X	X	X

Assessment conclusion

BSI assessment team

Name	Position
Wendy Fournier	Team Member
Gary Hull	Team Leader

Assessment conclusion and recommendation

The audit objectives have been achieved and the certificate scope remains appropriate. The audit team concludes based on the results of this audit that the organization does fulfil the standards and audit criteria identified within the audit report and it is deemed that the management system continues to achieve its intended outcomes.

RECOMMENDED - The audited organization can be recommended for certification / recertification / continued certification to the above listed standards, and has been found in general compliance with the audit criteria as stated in the above-mentioned audit plan.

Use of certification documents, mark / logo or report

The use of the BSI certification documents and mark / logo is effectively controlled.

Findings from this assessment

Scope and Access Management:

Planned activities have been fully realized. Methods for determining process results:

Overview of Office 365 Presentation

Office 365 Compliance Offerings - Suite of Cloud Based service offerings including our premier services (Exchange, Teams, SharePoint, Yammer, OneDrive, WAC), and numerous supporting services

Audit covers all locations worldwide

O365 licenses are sold by certified partners and MS affiliates

No changes in the previous year, original suite has not changed

No changes in the previous year to Context of the Organization. There were not any impacts due to Covid19 in the previous year.

Cloud Environment

IaaS - (Azure) All O365 is hosted on MCIO (ping, power, pipe, physical security and network management)

PaaS - O365 hosted using Azure (O365, EXO (Exchange Online), EOP (Exchange Online Protection))

EXO and EOP provide email capabilities, security features, reliability and management

- includes Spam identification and integrated AV

- O365 Cloud products includes, O365 Suite, WAC, OW, Teams, SharePoint, Exchange and EOP

SharePoint - information and documentation repository, that facilitates collaboration

Teams collaboration (IM, Audio calls, Video calls, online meetings, and web conferencing)

Access Control

Access Management Presentation February 2022

- Customer content isolated from service operations

- Task based privileged access model

- Minimal human touch

All customer content is treated as privileged, there is no standing access to customer content - least privileged access

- customer content is isolated from service operations - background check is required for access

- MFA

(Just in time access, Just enough access, time-bound, logging and auditing)

Multiple levels of approval for access, zero standing admin rights

Identity Federation

- Customers control authentication, per-user provisioning and de-provisioning, SSO, can use existing 2FA

Torus Tool - Account and Identity Management

Example, Employee asks for IDM, through Request, eligibility is verified and granted once approved

- Prior to authorizing, the profile is verified, background screening is verified, verify training has been completed, a EUPI attestation is completed

IDSS feed is synched, and via federation employee can access AD (file based RBAC Group Membership) through Lockbox RBAC approval Engine

O365 Account Access Workflow

O365 access through a request to the IDM portal (must be eligible first)

Approval is sent to manager, and workload owner must approve

Account is then provisioned

Accounts are renewed by sending a request to the IDM portal to request to reinstate access, and the same workflow is followed for provisioning access

If the employees manager changes, then access must be granted by the new manager (new manager must re-approve all employee access)

When an employee leaves the organization, IDM disables the employees' accounts

Lockbox - Access Control Management System, used to provision privileged access, is requested through Lockbox which sends request for approval, privileged access is timed Access is provisioned after approval from the Data Custodians

Customer Lockbox, option to extend lockbox prior to making request

Example of logs stored in Kubernetes of account provisioning requests sent to workload owner 20220214

Example M365 Identity and Access Management in Office 365 Substrate Pulse, example of logs on 20220214

Example User views eligibility in OSP (Office Substrate Pulse)

Eligibility does not allow an individual to make the request for a role that they do not perform

Request, elevates the permissions already eligible for

Examples of Account disabled notification email due to accounts that lost eligibility, 20220126 rlx, 20220207 you

EUPI handling of attestation (90 days) in Office 365 Substrate Pulse, for all employees who are eligible, attestation must be renewed every 90 days

Example of Accounts disabled after 35 days of inactivity, Employee Grixx, last login 20220105, eligibility removed 20220209

Employee Zhxx 20220225 all eligibilities removed due to inactivity

When the employee leaves the organization, access is removed immediately -

If they changed role, manager would have to re-apply

Elevated access after an account is provisioned 20220131, log of elevated access provisioned Email, 20220131 Lockbox Exchange Omxx CapacityFrontEndServer Admin Request Information, 20220131 Request Approved, 20210131 Action Executed Successfully

Planned results have been achieved.

Change Management A.12.1.2, A.14:

Planned activities have been fully realized. Methods for determining process results:

EXO & Substrate Change Management Overview, Principal Program Manager

There are two Change Management - Substrate Deployment Models (Model A (Central Admin CA), Griffin B-B2 (PilotFish PF))

Code Repository for Model A is Substrate, Control Plane and Griffin

Model B and B2 are Repositories populations in deployment populations with centralized evidence collection
148 compute services

Model A is the monolithic repository (deployed slower), Model B & B2 can be deployed faster

Model A uses regular train (2-3 weeks), Model B&B2 regular train is 1 week Fast

train is 1-2 days (A), and minutes to hours (B-B2)

Emergency train is 8-24 hours (A), 1-2 h or 30 min (B-B2)

PR (Pull Request) Code Review in Azure Dev Ops

Code Review Policies, automated check to ensure that the code review was compliant

Roslyn (static test tool)

Roslyn Results, demonstrates itemized root set (checking the roots that must pass) Hera
Build and Change Compliance Evidences 3

CCSServiceB2 Service using Azure build infra (cache credentials)

Code Review Policies, describe how many reviewers are required to review code

Deployment Regular Train, Build includes security testing and automated testing, Deployment includes monitoring Dogfood Testing

Separate instances of deployment includes SDV v2 (greater or equal to 24 h) and MSIT Ring (greater or equal to 4 days) and Worldwide Deployment (SIP Ring (greater or equal to 6 days), and Production, including GCQ))

Regular training indicates development is on schedule

Deployment Fast Train

- Can be deployed once the regular train changes have been deployed for urgent fixes
- Must be scope and applicable to the fast deployment or must take the regular train
- Requires GEM (Group Engineer Manager) to approve the change to be added to the fast train - Deployment to next stage within each ring starts as soon as previous stage has achieved desired saturation

Saturation of A is Stage 1 (50 machines or 1%), Stage 2 (250 machines or 5%), Stage 3 (100% of machines on branch)

Model B-B2 - Once scale unit at a time, to total 16 scale units

Model A Deployment, Regular Training (SDFV2 daily, MSIT Friday, SIP Tues, WW Monday), Fast Train (triggered by a FastTrain build), Emergency Patch (on demand)

Example Regular Train Model A halt example, 20210626 #247771704 Sev 1 Prod Dag, HubTransportAvailability Alerts, approved

Example of PR Code Review - 16.01 xxx, build 561xxx O365 Core Project, Griffin Repository, Roslyn - Pass

Example, Fast Train Model A - Approval 20210625 Use spark 2.4 for che & che01

Emergency patch (Model A) Approval sample, #249437188 20210707 Need to patch xxx

Example Model B-B2 Regular Train Rollback Request, #247695671 20210625 Service Recovery Rollback SIP

Emergency Situation - Safe Configuration Deployment #2314276596 20210311 Filter misconfiguration resulted in loss of xx

Roslyn Results Substrate Compliance example, CWA-web - server xxx

Hera Compliance Viewer - 6615 Deployment records, includes all of the fast train builds
Hera, internal tool to produce change management that connects different systems (Azure DevOps, Cosmos, Kusto, SQL, via Torus)

Hera Deployment Approval, example 20210507 Approved Lockbox Echange Bxxx- St Hera
PR Approval example, # 1333176 Add 100xxx to EOP backend IP space

CCSService B2 - Service Using Azure Build Infra

- 51 Deployments, 1 Service

Deployed builds example - 20200821 xxxmultitenant

Build Info - List of PRs example, Merged PR 561xxx, example of PR Approval, 20201009 Add mapping for exchange service unavailable

Code Review Policies include; Require a minimum number of reviewers, Check for linked work items, Limit merge types

Monitoring Criteria for halting deployment (Sev 1 alerts) Wiki Page 20210408 Example, #247771704 Dag HubTransportAvailability

Planned results have been achieved.

Vulnerability Scanning and Reporting A.12.6 Asset Management A.8:

Planned activities have been fully realized. Methods for determining process results:

Vulnerability Scanning and Reporting Presentation, February 23, 2022

PAPC Program for vulnerability management

- Vulnerability scanning across O365
- Qualys scanning tool is used (missing patches, application vulnerabilities, limited insecure configurations) - Results are aggregated and prioritized for triage via dashboards
- Remediation is measured with KPIs
- High Severity - patch release + 30 days, Medium - patch release + 90 Days (CVS Scale)
- Program is evaluated with 3rd party audits (ISO, SOC, FedRAMP)
- Scanning, Workload, Exception Approval Board are the 3 teams responsible for vulnerability patching

Scan Types include;

Agent (On and Off node scanning based on platform) + Qualys and Remote Network Scans (Qualys)

- Host snapshot creation, has metadata needed for vulnerability assessment, logs are stored in Geneva Service
- Vulnerability assessment is done by Qualys
- Remote scans target assets and interfaces that have out-of-band-management (OOBM) interfaces that cannot run a host agent

Architecture - Daily scans received from over 2 M assets and processed and displayed within 12 hour - Workload teams (own the servers), Azure runs Qualys scanner, PAVC team (manages the data)

Reporting - Internal Dashboard

- Prioritization by vulnerability and host
- The dashboard allows for filtering and on-the-fly calculations
- Default view shows items due or coming due by end of month
- Example 20220217 - 35 vulnerabilities (3 high, 2 med, 1 low outstanding by end of month)

Internal Dashboard, KPI Trending

- Measures non compliant vulnerabilities (20211012-20220217) range from 5- 31 depending on day - Non compliant host percentage - less than .5 %, daily from 20211211- 20211221

Internal Dashboard, Vulnerability Trending

- 50,000 detections to 2087 detections (95.8% fixed) within 1 week - 20220206 - 3% straggler hosts that were non-compliant

Central Admin - O365 Asset Management February 2022

- EXO Asset Lifecycle Management

- Central Admin Inventory Tracking (Hardware orders, new provisioned capacity and decommissioned hardware)
- New Orders - Delivered from GDCO ready for OS deployment, allocated to the new capacity forest
- Provisioning Ready for Allocation, allocated to new capacity forest - Provisioning Downloading Image, allocated to new capacity forest
- Pending Delivery (Awaiting Delivery from GDCO) (Asset Number (CA) = Asset Tag (GDCO)), and allocated to new capacity forest
- Live Assets inventory includes, assets with provisioning state, build information and role assignments - Decom - Hardware removed from DC, marked as removed
- Debug Role, Central Admin Orchestration via OSP, depicts various provisioning states

Planned results have been achieved.

Office 365 ISMS Management Review Clause 9.3 Context of the Organization Clause 4 :

Planned activities have not been fully realized. Methods for determining process results:

Office 365 ISMS Management Review Presentation - February 2022

External Issues include;

- Regulatory, Emerging regulations, PII Considerations, Industry Trends, Adversaries Internal Issues include;
- Service scale, Service Change Rate, Dependencies, Corporate context, Acquisitions

In the previous year, servers allocated to Teams increased significantly, email decreased with Covid-19, Supply Chain was impacted by Covid-19, Organization is acquiring DCs which feed all of Azure (O365 integrated with Azure)

Customer Requirements - Meet industry regulations, Customer requirements, Contractual Obligations, Trust
Management Requirements - Align with strategy, Consider risks and opportunities, Corporate culture
Engineering Requirements - Scalability, Ease of Implementation, Clarity

Leadership Commitment

- Enterprise Risk Management Program reports into Enterprise Management
- E&D Risk Management
- Business Continuity
- O365 Groups - Governance, Risks and Compliance, Security, Service Teams, Customer Experience

Enterprise Business Continuity, Internal Audit, Information Risk Management Council

Information Security and Privacy Objectives

Competence

- Job requirements, Candidate evaluation, Documented in the RecWeb tool

Competence - Evaluation

- Connect frequency depends on the rhythm of business
- Connect has 5 areas with room for employee and management

Example of Core Priority - Briefly state 2-5 Key Accountabilities

Evaluation example, Manage to grow a healthy productive and inclusive and diverse team

Example of Security Awareness

- Standards of Business Conduct (Achieve More)

Internal Communications: Service Updates, Roadmaps, MSRs, Planning Memos, All hands, Policy Example of email from leadership; 20220218 Reminder about our security and privacy policies and resources

External Communications: Service Health Dashboard, Blogs, Technet, TrustOffice, Audit Reports, Contracts, Customer Service

- Assessment Reports, Admin Center, TechNet, Service Trust Platform, Office Support

Documentation

-Key Documentation stored on SharePoint (Office 365 Information Security Policy, MS Privacy Policy, O365 Control Framework, Statement of Applicability, Risk Management Program, Remediation Program, ISO 22301:2019, 27001:2013, 27017:2015, 27108:2014, 27701:2019, NIST 800-53))

- Documentation is stored on SharePoint sites and updated as necessary

Operational Planning and Control includes: Evaluating the operation of controls (through continuous monitoring, internal audit, enterprise risk management, third party audits), Service team change management, New team onboarding

Monitoring activities include the measurement of the following activities:

Patching, Configurations, Anti-Malware; Competence, Overall Control design and implementation, User Access, Incident Response, Capacity, Disaster Recovery

Internal Audit include audits by the following organizations: -

MS Internal Audit, FedRamp, SOC

Nonconformity Remediation Process

Continual Improvement

- ISMS reviews cover suitability of control design and effectiveness to meet objectives - Control Design & Control Effectiveness

20220202 ISMS and SOA Review Meeting Minutes, review and approval of the ISMS and SOA for O365

Planned results have not been achieved.

ISO 27017 Controls :

Planned activities have been fully realized. Methods for determining process results:

ISO 27017 Presentation, February 2022

MS provides guidance on how clients should assign admin access in Admin Center
Geopolitical location and information is on the Admin Portal, company profile
MS communications the roles that exist for Customers and how it can be configured White Paper describes tenant isolation controls in O365

CLD 6.3.1 Shared Information security roles

- MS communicates customer roles and suggests how to configure admin roles
- MS has published several white papers to explain how it manages the environment, example, Security in Office 365 - Tenant Isolation in Office 365

CLD 7.2.2 (Training and Awareness) and CLD 8.1.1 (Asset Management Data Identification) covered in ISO 27001 interviews

CLD 8.1.5 Asset Management and Termination- Assets should be removed and returned to the customer in a timely way when the cloud service agreement is terminated.

CLD 8.2.2 Data Classification - MS treats all client data as restricted data, as described in the MS Data Handling standard

Customers can classify (label) their data with retention and sensitivity labels from the Home tab on the ribbon

MS Trust Center page, You Control Your Data

CLD 9.2.1 User Registration and Deregistration - User creation and deletion functions Article

- Set up MS 365 for Business 20211005

Client manages licenses from the Admin Center

User registration and deregistration, also supports alternative solutions, for example federation of accounts

White Paper, Controlling Access to Office 365 and Protecting Content on Devices, July 18, 2016, provides detailed information for client set up

MS Admin Center Documentation, article 20220210 - Set up Multifactor Authentication

CLD 9.2.3 Enhanced Authentication - O365 supports 2FA and supports federated authentication, customer owns end to end authentication and authorization process

MS Admin Center Documentation, article Cloud Identity Password Management

CLD 9.2.4 Secret Management - MS Admin Center Documentation provides password policies to manage user authentication secrets. O365 does not have access to clear text information of customer secrets

CLD 9.4.4 Sensitive Utility Programs - customers cannot bypass normal operation or security procedures

CLD 9.5.1 Virtual Environment Segregation - MS Admin Center Documentation, Isolation Controls - MS Service Assurance (Tenant Isolation). MS does not run customer services and therefore does not isolate customers from one another

CLD 10.1.1. Cryptographic Usage - All customer communication requires encryption. Customers can control their lockbox, enable message encryption, and use rights management

White Paper Data Encryption Technologies in Office 365 is available in the Trust Center

CLD 11.2.7 Secure Disposal and Reuse of Equipment - managed by Azure Infrastructure

CLD 12.1.2 Operations Security Change Management - Updates are published on the Admin Portal Example, 20211022 Message # MC151939 New Feature Add MS Teams to existing...

CLD 12.1.3 Operations Security Capacity (covered by ISO 27001)

CLD 12.3.1 Backups - Data is duplicated based on the redundancy zone(s) it is assigned to. It is always duplicated, but not duplicated to every data center. Most zones are pairs with potentially additional colo's in the DC's to increase redundancy

Admin Center article, Data Resiliency in MS 365 20211117

CLD 12.4.5 Cloud Monitoring functionality - O365 management activity API

CLD 12.6.1 Vulnerability Management (covered by ISO 27001)

CLD 13.1.3 Network Segregation - Designed with service layer isolation

CLD 13.1.4 Virtual and Physical Network Consistency - Designed for security and encryption

CLD 14.1.1. Information Security Capabilities - Security Commitments to customers is documented in the Online Services Data Protection Addendum (Behind the Scenes, Securing the Infrastructure Powering the MS 365 Services)

CLD 14.2.1 Secure Development Procedure - Secure Engineering DevOps is published on the Admin Center

CLD 15.1.2, 15.1.3 Supplier Relationships - MS has a Global Supplier Program (How to do business with Microsoft)

CLD 16.1.2 Security Event Reporting and Tracking - MS provides a portal for anyone to report and track a vulnerability. Customers are notified of security issues in the portal and pen-test completed by a third-party vendor is published on the portal.

CLD 18 Compliance (covered by ISO 27001)

Planned results have been achieved.

Operations Security:

Planned activities have been fully realized. Methods for determining process results:

ISO 2022 Audit Teams, Operations Security

Documented Operating Procedures are stored on Wiki

- Teamspace wiki
- Example of Deployment Process, reviewed revision history 20220211

Capacity Management CPU, thresholds are determined by the various teams

- Geneva data collection from Jarvis tool managing threshold
- Red alerts sent out via ICM, if red for sustained period of time on call teams manage alerts
- # 292187823 20220301 CSA Resource Health, the issue auto-resolved

Azure subscriptions are used to manage the various environments - testing and dev are non-prod, which is completely separate

Azure security pack provides anti-malware controls

Azure geo-redundant storage (primary example, Arizona and secondary is Texas)

ICM is the alerting mechanism, for monitoring

Logs are maintained in ICM

Logs are protected HOSTIDS and sent to Vanquish via Geneva

Admin and Operator logs are done the same way, logs are

Azure is used for clock synchronization using UTC

Installation of Software on Operational Systems

Azure Dev Ops RM is used to push out updates

Restriction on Software Installation - Second reviewer required to check in code, after all quality gates have passed. Requestor and approver are required for ADO release

A developer must have a second reviewer

Lockbox checks requestor and approver for each release

Planned results have been achieved.

Human Resources Security & Supplier Management Standard A.7 - A.15:

Planned activities have been fully realized. Methods for determining process results:

Office 365 Human Resources Security & Supplier Management Standard - March 2022

Background screening required of all employees and vendors

-Hire Right is used for screening (background check) (education, employment, criminal, and credit, general reputation and personal characteristics) + US Citizenship Verification, Fingerprinting, PTP-M, PTP H, CJIS, DOD, IT 1&2 (US Government Cloud)

- Vendor or FTE request background screening through IDM, FTE screening results are returned to Microsoft

- Subjective assessments made by legal for FTEs who don't pass, Vendors are required to have a pass - Screening data is stored in MS SAP, terminated employees records maintained 5 years

MS Security Policy and Standard, are available to all employees

Required FISMA Training (Privacy and Security Foundations) and Code of Conduct

Terms and Conditions of Global Employees: Non-disclosure Policy, Security Policy, Policies for External Staff, Employee Handbook

Non-disclosure stored on HRweb SharePoint , 20211216 Employee

Handbook available on MS website

HRweb has policies

Disciplinary Process, Termination & Change of Employment

FY21 Supplier Management Standard 20210416

- Supplier list is published externally, 6 months in advance (GDPR) - Human Resources are the main suppliers relevant

Teleworking - Hybrid Workplace Flexibility (HWF) Guide (policy)

Planned results have been achieved.

Subscription Termination:

Planned activities have been fully realized. Methods for determining process results:

- If tenant decides to leave the service
- Review of logs in Kusto Explorer 20210608, status can be Suspended, LockedOut, Active
- Code snippet of configuration, trigger absolute deletion on day 25
- Information is permanently deleted after day 25 (once deletion has begun, there is nothing that can be done)
- Example 20210701 customer log FWDSync
- The same process is applied for voluntary and involuntary terminations

Planned results have been achieved.

Office 365 Compliance -A.18 :

Planned activities have been fully realized. Methods for determining process results:

Office 365 Compliance - ISO Audit 2022 Presentation

New requirements are identified by CELA (Customer Experience), Field, and CXP and are triaged according to customer need, and the effort to implement

- Requirements are analyzed and new documentation and control frameworks are updated
- New requirements are onboarded and implemented
- Currently rolling out Germanys C-5

Intellectual Property Rights - Policies include; Using Third Party Content, Notice & Takedown for copyright, trademark & publicity rights, Third Party Software Governance, Microsoft Open Source Docs, Report Possible Infringement

Protection of Records

- Data types are assigned to address retention, transmission, storage, use limitations, sharing with 3rd parties, allowable customer communications, encryption requirements, connected apps, telemetry

- Various data types include; access control data, customer content, end user identifiable information, support data, account data, public personal data, end user pseudonymous information, organization identifiable pseudonymous, system metadata, public non-personal data, security logs

Independent review of information security through internal audits, ISO, FedRamp, SOC2, Enterprise Risk Management

Compliance with security policies, Risk Review Meeting Jan 26, 2022 and Office Hours Summary Notes Feb 10, 2022

Technical Compliance Review includes Penetration Testing, Patching, AV and PAVC Scanning, External Third Party Vulnerability Assessment, Coalfire example 2021

Planned results have been achieved.

Cryptography - Protocols and Cyphers :

Planned activities have been fully realized. Methods for determining process results:

Policy - Protecting customer data from government snooping

Weak Protocols

Examples, SSL (deprecated in O365 for several years)

Weak Cyphers

- minimum lengths 112 bits and minimum 128 bit key length

Insecure renegotiation

- SSL TLS protocols support ability to renegotiate an existing connection

Weak Hashing Algorithm

- Most certificates use SHA1 hashtag

Protocol Support requirements

All computers must comply with PCT 1.0, SSL 2.0, 3.0 must be disabled

TLS 1.2 must be enabled

Service must disable insecure renegotiation

Detection and alerting system scans endpoints to detect unauthorized protocols, Service 360

Example 20210601 Uses TLS 1.2 and remove support (assigned to OS)

Example 20210630 Remove unsupported Cipher Suites

Cipher Suite Requirements

Weak and medium ciphers must be disabled, only PFS (Perfect Forward Security) is allowed

Key Management

- All symmetric keys have maximum 3 year lifetime, recommended 1 year lifetime
- Root CA certificates (RSA key length must be 4096 bits or more, ECC key must either P-384 or P-521 curves, certificate must not exceed 25 years)

HTTP Strict Transport security is enabled

- requirement for HTTPS connections
- clients use HSTS by providing Strict Transport Security header in the HTTP response field

Example TLS Tracking Sheet, for Skype

Planned results have been achieved.

ISO 27701:2019, 27018:2019:

Planned activities have been fully realized. Methods for determining process results:

ISO 27701:2019, 27018:2019 Privacy Controls Presentation March 2022

ISO 27018 main presentation deck

A.2.1 Consent and Choice; Obligation to co-operate with PII principals rights

- Cloud customers have control of their own data to access, correct, and erase customer data through the Admin Portal and IW Portal Settings
- Customers can use the Azure Portal to fulfill their end user GDPR DSR requests (Welcome to Microsoft Cloud Services User Privacy Experience)

A.3.1 Public Cloud PII Processors Purpose

A.3.2 Public Cloud PII Processors Commercial Use

- MS Product Terms and DPA, client data used for to improve MS offerings, Business Operations (6 categories) , and security, but does not use client data for commercial and marketing uses (customer data is only used for legitimate Business Operations, Compensation, Internal reporting (capacity planning), fraud, cyber-crime, and to improve core functionality and financial reporting and compliance
- MS Product Terms and MS Products and Services Data Protection Addendum (DPA) clauses: Nature of Data Processing: Ownership, Processing to Provide Customer the Products and Services, Processing for Business Operations, Processing of Personal Data - GDPR
- Data Handling Standard enforces contractual requirements for not using Customer Data for advertising and commercial purposes
- Data Access Request review ensures data use of personal data meets allowable use requirements

A.5.1 Data Minimization

- Temporary files are erased and destroyed within a documented period (when patched every month)
- Temp files created by OS are cleaned up by OS
- Temp files created by services, temp files are cleaned up when session ends
- If the session ends abnormally, temp files are cleaned up by the garbage collection process

A.6.1 PII disclosure notification

- MS Products and Services Data Protection Addendum
- If customer leaves service, data is maintained for 90 days (opportunity to change mind and recover data)
- Customer data is not disclosed to third parties unless directed by customers or required by law
- Third party requests for data are managed by MS Law Enforcement and National Security Global Fulfillment
- Microsoft publishes MS Law Enforcement and National Security Global Fulfillment (aggregated)

A.8.1 Disclosure of sub-contracted PII Processing

- MS Products and Services Data Protection Addendum
- List of sub-contractors is published on MS Trust Center, if sub-contractor access client data (6 month in advance), clients can receive a notification if there is a change to the list

A.10 Accountability

- O365 Security and Privacy Incident Response SOP
- Notifications of data breach involving PII (GDPR requirement) to customers and relevant authorities within 72 hours
- Notification is published on the MS Message Center, some customers are notified by email
- Policy on document retention schedule is published internally
- Customer data is retained for 90 days when the subscription expires
- Data at rest and data in transit for EU customers
- O365 Data Handling Standard
- Confidentiality and NDA Policy, every employee signs and NDA and is obligated to maintain confidentiality Business Code of Conduct is attested to every year

A.11 Restriction of the Creation of Hardcopy Material

- Prohibited to connect printers and portable media in DC
- Access to Customer Data is strictly controlled
- Customer data is restricted no creation of hard copies or printing and copying
- MS Security Policy on Asset Management for destruction of hardcopy materials - Customer data is continuously replicated, in the same geo-dispersed center
- Recovered data is logged, if outside of the recovery window they have to contact Microsoft through support ticket
- MS Security Policy prevents data on storage media from leaving the premises
- Portable storage devices is prohibited

- Customer data is encrypted at rest and in transit, and allows for encryption in transmission FIPS-140-2 validated ciphers
- Connection to customer is between FIPS validated TLS protocol
- Secure disposal of hardcopy material, is according to record management policy and retention policies schedule
- Unique user IDs is through Azure which enforces unique identifiers, and authenticates unique users - Record of authorized users - control of personnel who have authority to access systems based on their role

JIT tools enforce granular conditions, no one has standing permissions

- AD enforces the unique identifier
- Contract measures for unlawful access - Security Measures - Commitment
- Sub-contractors sign MS Master Service Agreement, must register in SSPA and sign the DPR

Access to data on pre-used data storage space

- Customer data is encrypted
- Segregation of data is through AD and AAD

A.12 Geographic location of PII

- Geographical location of PII, where data is stored (DC locations, and city locations)
- O365 relies upon internet protocols and encryption to ensure data reaches its destination
- Encryption prevents unauthorized disclosure
- FIPS 140-2 ciphers are used for integrity validation for customer, interconnected system and remote access connections
- Relies on internet protocols and encryption (TLS over TCP) to ensure data reaches its intended destination

ISO 27701:2019 Privacy Information Management for PII Processor - March 2022

B.8.2.1 Customer Agreement

- Privacy principles (additional control not covered by 27018 is Data Protection Impact Assessment) BPIA updated annually (MS policy needs annual updates) - Required for all customer data and personal data processing follows requirements of GDPR

B.8.2.2 Organizations Purposes - covered by ISO 27018

B.8.2.3 Marketing and Advertising Use - covered by ISO 27018

B.8.2.4 Infringing Instruction

- MS does not provide legal advice, and customer is responsible for controlling their data (MS is the processor, not controller)
- MS redirects data requests to customer, unless prohibited by law
- End user should go to data controller to make the request

- Data breach, notification within 72 hours

B.8.2.5 Customer obligations

- MS provides customers information about O365 services compliance
- MS Trust Center, Customers can get information about Security, Privacy and Compliance
- Service Trust Portal - provides audit O365 audit reports and risk assessment guides
- Compliance Manager - Risk assessments of MS Cloud and customer compliance activities per international and regional compliance requirements
- Security and Compliance Center - Data governance and data protection
- Public facing documentation for assessing MS Cloud services for their role as data controller

B.8.2.6 Records Related to Processing PII

- Contractual is covered by DPA on Disclosure of processed data
- Data access requests records are stored in ICS
- Just in Time Access elevation request logs

B8.3.1 Obligations to PII principles

- Tenant Admin acting on behalf of end users (accept product terms, contractual commitment)
- Provide information to assess risks of using MS services (Service Trust portal)
- Through Azure Admin Portal they can provide their organization privacy statements and manage their users and groups
- End user can also see MS privacy statements
- Admin can control O365 products (on off, opt in and out, configuration settings, policy settings) - Privacy management feature to search content in their documents and emails for private data, and delete the data (for E5 customers), released last year
- Excellent product for example, Bank loan documents

Additional controls are covered by ISO 27018

B 8.4.1 covered 27018

B 8.4.2 covered 27018

B 8.4.3 covered 27018

B.8.5.1 covered 27018

B.8.5.2. 27018 - commit to comply with contractual clause

MS complies to the standard that is the most stringent and map the rest of them.

Planned results have been achieved.

Risk Management :

Planned activities have not been fully realized. Methods for determining process results:

O365 Risk Management February 2022 Presentation

Compliance Lifecycle is a federated effort

- Lifecycle includes market intelligence, regulatory impact, defining security and privacy controls, implementation requirements, implementation of controls, documentation, continuous monitoring and testing, independent verification (audits), assurance risk and remediation

Risk Program Goals and Benefits

- Risk Management as a Differentiator (supports scale and agility, Strategic Enablement to unblock accreditations and generates trust, Engineering Focused, Provide Transparency

MS 365 Risk Flow

Inputs to Risk from the following teams

- Security, BCM, Identity, Trust
- Risk from EXO, SPO, MS Teams, Service Teams - Internal Audit, Board of Directors

Process Outputs

- Identify New Risks, Assess Risks, Develop Treatment Plans, Report Status to Management, Monitor Review Risks

Identify New Risks through Internal and External Audit Findings, Continuous Monitoring Findings, Pen Tests, Vulnerability Scans, Active Security and Compliance Exceptions and Remediation Work, Trust GRC, Workload, Partner Interview and Workshops, Risk Register

- Assess Risks based on Impact, Likelihood, Control Opportunities Scale from 1- 5, multiplied to have severity score
- Risk owner is assigned and treatment option agreed (Accept, Treat (control transfer avoid)) ADO Azure Dev Ops tool is used to record risks

Risk Assessment and Report of status, yearly presentation to management

Risk Management Plan is updated yearly (meet with risk owners, update treatment plans, reassess risks)

Key Discussion Objectives are to Support a risk-aware culture, Identify and manage cross Enterprise risks, Enhance enterprise risks response decisions, Reduce operational surprises, Identify new opportunities, Provide transparency to key stakeholders

Key Discussion Points include, Assessment for enterprise risks, Challenge impacting strategy, New and emerging risks, Progress on management actions, Changes in external and operating environment, Management incorporates into their enterprise risk discussion

Example #240485 Risk Owner Review Oct 1, 2020 to Sept 30, 2021, status date 20210630

Planned results have not been achieved, but are proceeding and being actively managed.

Remediation and Exception:

Planned activities have not been fully realized. Methods for determining process results:

Remediation Team remediates audit findings from annual findings

- Track and monitor FedRamp (table 4.1), SOC and audit findings
- Prevention (SOC and enforcing ST review)
- Report to customers monthly, document and track in ADO

Findings are tracked in the Remediation Dashboard

- New, Active and Approved Findings - 29
- Changes made by non Remediation Team - 10
- Recently closed - 3
- Internal Audit 36
- Past Current Target date - 17
- Approved FedRAMP by environments- 39
- Outstanding ORs and Findings 68
- Outstanding OR (including legacy) 55

Delays to close, High 30 days, Medium 60 days, Low 120 days

Ado Ticket examples

Remediation Sample #224799 20200730 Server password policy - password length, set to minimum length 14 characters

Exception

- Short term time extension to resolve non compliance, KPI or security issue
- Team gathers information for approvers and monitors commitments
- Exceptions are granted on variable time frame
- Exception Dashboard in Trust Compliance
- New Exception Requests Dashboard 14, GDPR by Stage 32, DataBricks by State 12, Privacy Review by State 7, Security Review by State 7, All Exceptions by State 169, TLS Exceptions by State 14, BCM Exceptions by State 8, IDEAs Exceptions by State 14, Exemptions by State 5
- Example of Exception Item #161590 20191010 Exception SIP - Prevent engineers from self-approving Lockbox requests

Planned results have not been achieved.

SRT (Security Response) Security Response Team:

Planned activities have been fully realized. Methods for determining process results:

Security Response Team (SRT-IR) Presentation March 2022

Federated Security Response Model

- Detection and Analysis
- Containment, Eradication and Remediation
- Post Incident Activity

SOP NIST 800-61 Based Response Process

- Preparation, Detection & Analysis, Containment Eradication and Recovery, Post Incident Recovery

Onboarding of New Services includes - SOP Team Process, Services Guide

Federated Partner Guidance

- SIR SOP Published Annually, annual review of team updates by federated partners - Current version 2022.01 20220207

Battlecard provides Security Guidance (Important points to remember for example, contact number and help to fill out the forms)

Role is Protection of the service M365

Examples of ICM ticket, automatically has a SLA

#286960123 20220203 Compromised email addresses received

#289074704 20220214 CDOC SSRIP ticket opened

New Employee Onboarding

- SOP NEO- OCE Quick start checklist for new hires
- Mentor signs off on new trainees

Example of New Employee Signoff Records, #1846696 CY19 SRT Neo (Master) #

2317171 New Hire is OCE Ready Q4CY 21-11

Incident Response Team is made up of Lead Investigator, Incident Manager, Security Incident Manager, Communications Manager, Subject Matter Experts

Security Response Process

- Triage (severity, Impact, Summary, NTK needed)
- Investigate (Containment, Remediation, Artifact Collection, TI Sharing)
- Classify (Security Incident, Breach or Privacy Impact, True Positive or False Positive)

- Continuous Improvement (Post Mortem, Engineering Fixes and Repair Items, SRT Work Items and Bugs)

Scope & Classify - Iterative Process to Analyze, Assess, Impact and Scope

- Classified as False Positive or Escalation, Security Incident, Privacy Impact, Customer Data Breach - Customer Data Breach is the most severe

Reporting Security Issues

- SLAM Detections, Human Analysis & Observation

Cloud Security Incident Response- Customer Perspective

O365 is mostly SaaS, running on servers throughout the world

- Tenant sitting on top of platform, if they give a tenant and you leave the windows of your car open - MS does not monitor for that, Shared Responsibility model

Detection and Analysis

- Triage, Investigate, Scope and Classify (true or false positive)

ICC Team owns communication to customers and MS executives (communication and risk escalation)

Q4FY21 - 12 Customer Communications related to breaches (12 individual customers)

Post Incident - Post Mortem

- Required if there was a customer notification
- ServiceNow PIR Playbook 20180919

O365 SIR - Investigation Types

- Service, Vulnerability, Tenant, Abuse-Fraud, Data Loss, Privacy
- Example, Service Now Playbook 20180919

Planned results have been achieved.

Yammer :

Planned activities have been fully realized. Methods for determining process results:

Yammer Security, Privacy & Compliance Overview March 2022

All Azure subscriptions are on Torus (M365 tenant), Azure resources management follows M365 Process (OSP Portal, Yubikeys, etc)

- Using Secure Access Workstations
- Authenticated using AD
- Used to communicate (leadership engagement, communications knowledge sharing, employee experience)

- Yammer Architecture, EU clients access through Azure EU customer route, all other customers use Azure US route (AzureFD)
- Data cannot migrate from US to EU, EU must start as EU customers (start fresh)
- Yammer manages infrastructure except for top licensing layer with M365
- Yammer is isolated from the rest of MS, requires Yammer VPN (no access from MS networks) and Yammer 2FA
- Access is Just In Time, OSP Torus Client
- O365 customers create and delete functions to provision access
- Yammer Engineering team, onboarding and off-boarding for access, need to be authorized to access Yammer and have Yammer credentials
- Yammer employees onboarding to Yammer Infrastructure team must request access, account is federated and authenticated with Yammer LDAP services - Production access passwords are reset every 70 days
- Yammer LDAP account creation workflow requires security approval
- Example 20220120 request for Yammer access for employee DQ, approved by security team
- Once the individual has LDAP access, they can request privileged access if required
- Request is through the Compute group for approval (identity, Cloud Background Check, and required training verified prior to approval) prior to adding the account to the production access group
- Example Request from manager BP 20220215, review of background check completed 20220216, evidence of required training was reviewed (Trust Conduct, Privacy Fundamentals, Security Foundations)
- Enhanced authentication is 2FA through O365
- LDAP password rules apply, minimum MS requirements (10 characters, Uppercase, Lowercase, a number, a special character, password match) - passwords are changed every 70 days
- Privileged accounts are reviewed every 3 months, Security Team monitors changes on privileged LDAP groups
- Ldap diff tool, Homie3 Authorizers List, Azure subscriptions, Azure devops security groups automated tools to monitor access Example of review tasks
- #182812 Task Project Collection Administrators February 2022
- #183814 Project Collection Administrators Azure DevOps February 2022
- #183812 Yammer infra Torus Team Review February 23, 2022

Removal of Access Rights, termination by HR team, goodbye post

Example, 20220224 Offboarding for Monday Feb 28, 2022 from employee MB

Example, 20220112 Offboarding Left Microsoft (removed LDAP, Yammer AAD, PagerDuty, Wavefront)

Information Access Restriction, example duration 1 hour - Homie3 tool provisions privileged access on time limited basis with approval from engineering managers and tech leads - Maximum access through this process is 7 days

Use of Privileged Utility Programs, all activity is logged and monitored -
Customer usage is not monitored

Azure DevOps is used for development, build release and hosting of source code, restricted to Yammer team

Operations A.12

Operating procedures are documented in Azure DevOps, Yammer Policies and Procedures Examples, Yammer Access Control Procedure, Yammer Change Management Procedure, Logging and Monitoring, Security Incident Response Plan, Security Policy, Logging and Monitoring Procedure

- Procedures were reviewed 20220222, Security team does final reviews and approvals

Example of annual review #91856 Yammer Procedures Policies yearly refresh and review

Yammer Engineering Wiki pages for knowledge articles, lessons learned, runbooks Example, Architecture Specs and Reviews

Change Management process includes Build, Release, Deploy phases

- changes are documented and tracked in Azure DevOps
- Pull request for a service Change and Release example #39463 20220213 Updated CPU and instances based on usage

Yammer uses the MS 365 Admin Center

Capacity Management

- Yammer plans capacity through a monthly meeting (Monthly Service Reviews) to forecast and predict capacity and data included in M365 MSR meetings

Example, MSR Jan 2021 includes Yammer capacity (evidence of all monthly MSR)

Examples All Incidents November 2021 listing

- #161768 Edgexxx 20211125 Critical situation (mitigated)
- #161765 CFL New xxx 20211125 Urgent (closed)

Separation of Environments

- Yammer has separate pre-production (staging), development with shared LDAP directory with their own VPN, and are in different Azure subscriptions
- Labs do not connect to staging or production
- Example, Release 486 - verified

Malware

- Protected through open source tool called Sysdig Falco
- Intrusion detection rules are enabled - verified (examples, launge sensitive mount container, docker client is executed in a container, system procs network activity)
- Intrusion detection has 100% coverage - verified

Backups

- Azure snapshots of disc db and write ahead log (point in time)
- Azure DevOps backup daily
- Can restore real time data

Logging and Monitoring

- authentication requests, security and OS system events, source addresses, exceptions, suspicious events and alarms are logged and monitored
- logs are on Yammer Kusto, Security Posture Dashboards, and Queries in LensUI
- OS and security logs are maintained for 365 days (forensic and audit purposes) and service logs for 30 days
- Metrics are in Wavefront Yammer
- Access to logs is restricted and via Yammer KustoUsers Security Group - All activity by Yammer engineers is tracked

Clock Synchronization is through Azure

Installation of Software on Operational Software

- Docker Base Image and any other software is applied on top of the base image
- any additional software must be approved

Example 20220218 #91064 Updating with latest Java 8,11,17

Vulnerabilities

- part of O365 pen testing, and findings tracked in Yammer Azure DevOps
- vulnerability scans are done comparing to Anchore-Engine tool (will transition to 1ES Component) - vulnerabilities tracked using M365 Security Bugs Policy

New and Archived Audit Reports on Service Trust Portal

Audit Controls Reports are stored on the Azure DevOps and SharePoint

Access is through Yammer VPN, Access to containers is logged

Example 20220222 user tpoxxx accessed prodxxx

Network Segregation for customer is through tenant isolation

Yammer BCM test is conducted yearly by Yammer, last exercise was in May 2021

Planned results have been achieved.

Next visit objectives, scope and criteria

The objective of the assessment is to conduct a surveillance assessment and look for positive evidence to ensure the elements of the scope of certification and the requirements of the management standard are effectively addressed by the organisation's management system and that the system is demonstrating the ability to support the achievement of statutory, regulatory and contractual requirements and the organisations specified objectives, as applicable with regard to the scope of the management standard, and to confirm the on-going achievement and applicability of the forward strategic plan.

The scope of the assessment is the documented management system with relation to the requirements of ISO 27001, ISO 27017, ISO 27018, ISO 27701 & ISO 22301 and the defined assessment plan provided in terms of locations and areas of the system and organisation to be assessed.

ISO 27001, ISO 27017, ISO 27018, ISO 27701 & ISO 22301
Microsoft 365 management system documentation

Please note that BSI reserves the right to apply a charge equivalent to the full daily rate for cancellation of the visit by the organization within 30 days of an agreed visit date. It is a condition of Registration that a deputy management representative be nominated. It is expected that the deputy would stand in should the management representative find themselves unavailable to attend an agreed visit within 30 days of its conduct.

Next Visit Plan

Date	Auditor	Time	Area/Process	Clause
------	---------	------	--------------	--------

Appendix: Your certification structure & ongoing assessment programme

Scope of Certification

IS 552878 (ISO/IEC 27001:2013)

The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII) in accordance with the Statement of Applicability dated February 19, 2020.

PII 663484 (ISO/IEC 27018:2019)

The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII) in accordance with the Statement of Applicability dated February 10, 2020. (ref. ISO 27001:2013 certificate number IS 552878).

CLOUD 663485 (ISO/IEC 27017:2015)

The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII) in accordance with the Statement of Applicability dated February 10, 2020. (ref. ISO 27001:2013 certificate number IS 552878)

BCMS 706252 (ISO 22301:2019)

The business continuity management system in relation to the availability of Microsoft Office 365 services.

PM 741035 (ISO/IEC 27701:2019)

The Privacy Information Management System applicable to Office 65 Privacy Information Management System Development, Operations and Support in accordance with the Statement of Applicability dated February 19, 2020. (ref. ISO 27001:2013 certificate number IS 552878).

Assessed location(s)

The audit has been performed at Central Office.

Redmond / IS 552878 (ISO/IEC 27001:2013)

Location reference	0047358928-001
--------------------	----------------

Address	Microsoft Office 365 1 Microsoft Way Redmond Washington
	98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3322498
Assessment dates	03/02/2022
Deviation from Audit Plan	No
Total number of Employees	26
Total persons doing work at this site	26
Scope of activities at the site	The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII) in accordance with the Statement of Applicability dated February 19, 2020.
Assessment duration	2.5 Day(s)

Redmond / BCMS 706252 (ISO 22301:2019)

Location reference	0047358928-001
Address	Microsoft Office 365 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3361974
Assessment dates	02/28/2022
Deviation from Audit Plan	No
Total number of Employees	26
Effective number of Employees	26

Scope of activities at the site	The business continuity management system in relation to the availability of Microsoft Office 365 services.
Assessment duration	2 Day(s)

Redmond / CLOUD 663485 (ISO/IEC 27017:2015)

Location reference	0047358928-001
Address	Microsoft Office 365 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3436208
Assessment dates	03/01/2022
Deviation from Audit Plan	No
Total number of Employees	26
Effective number of Employees	26
Scope of activities at the site	The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII).
Assessment duration	1 Day(s)

Redmond / PII 663484 (ISO/IEC 27018:2019)

Location reference	0047358928-001
Address	Microsoft Office 365 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3436207

Assessment dates	02/28/2022
Deviation from Audit Plan	No
Total number of Employees	26
Effective number of Employees	26
Scope of activities at the site	The management of Information Security Management System (ISMS) for Microsoft Office 365 Services development, operations, support, and protection of personally identifiable information (PII).
Assessment duration	1 Day(s)

Redmond / PM 741035 (ISO/IEC 27701:2019)

Location reference	0047358928-001
Address	Microsoft Office 365 1 Microsoft Way Redmond Washington 98052-8300 USA
Visit type	Continuing assessment (surveillance)
Assessment number	3504167
Assessment dates	03/02/2022
Deviation from Audit Plan	No
Total number of Employees	26
Total number of persons with access to PII	26
Total number of PII records	100000
Scope of activities at the site	The Privacy Information Management System applicable to Office 65 Privacy Information Management System Development, Operations and Support in accordance with the Statement of Applicability dated February 19, 2020. (ref. ISO 27001:2013 certificate number IS 552878).
Assessment duration	3 Day(s)

Certification assessment program

Certificate Number - IS 552878

Location reference - 0047358928-001

		Audit1	Audit2	Audit3
Business area/Location	Date (mm/yy):	02/22	02/23	02/24
	Duration (days):	9.5	9.5	12
ISMS Changes + ISMS Scope Review		X	X	X
Context of the organization		X	X	X
Information Security Policy		X	X	X
Information Security Objectives		X	X	X
Competence, Awareness, Communication		X	X	X
Information security risk assessment, information security risk treatment, and Statement of Applicability (SOA)		X	X	X
Documented information		X	X	X
Management Review		X	X	X
Internal Audit		X	X	X
Nonconformity and Corrective Action		X	X	X
A.5 Information security policies		X	X	
A.6 Organization of information security		X	X	X
A.7 Human resource security		X	X	
A.8 Asset management		X	X	X
A.9 Access control		X	X	
A.10 Cryptography		X	X	X
A.11 Physical and environmental security		X	X	
A.12 Operations security		X	X	X
A.13 Communications security		X	X	

A.14 System acquisition, development, and maintenance	X	X	
A.15 Supplier relationships	X	X	X
A.16 Information security incident management	X	X	
A.17 Information security aspects of business continuity management	X	X	X
A.18 Compliance	X	X	

Certificate Number - PII 663484

Location reference - 0047358928-001

		Audit1	Audit2	Audit3
Business area/Location	Date (mm/yy):	02/20	02/21	02/22
	Duration (days):	1.0	1.0	1.0
A.1 General		X	X	X
A.2 Consent and choice		X	X	X
A.3 Purpose legitimacy and specification		X	X	X
A.4 Collection limitation		X	X	X
A.5 Data minimization		X	X	X
A.6 Use, retention and disclosure limitation		X	X	X
A.7 Accuracy and quality		X	X	X
A.8 Openness, transparency and notice		X	X	X
A.9 Individual participation and access		X	X	X
A.10 Accountability		X	X	X
A.11 Information security		X	X	X
A.12 Privacy compliance		X	X	X

Certificate Number - CLOUD 663485

Location reference - 0047358928-001

	Audit1	Audit2	Audit3
--	--------	--------	--------

Business area/Location	Date (mm/yy):	02/20	02/21	02/22
	Duration (days):	1.0	1.0	1.0
CLD.6.3.1 Shared roles and responsibilities within a cloud computing environment		X	X	X
CLD.8.1.5 Removal of cloud service customer assets		X	X	X
CLD.9.5.1 Segregation in virtual computing environments		X	X	X
CLD.9.5.2 Virtual machine hardening		X	X	X
CLD.12.1.5 Administrator's operational security		X	X	X
CLD 12.4.5 Monitoring of Cloud Services		X	X	X
CLD 13.1.4 Alignment of security management for virtual and physical networks		X	X	X

Certificate Number - BCMS 706252

Location reference - 0047358928-001

		Audit1	Audit2	Audit3
Business area/Location	Date (mm/yy):	01/20	02/21	2/22
	Duration (days):	1	1	2
Scope and Policy		X	X	X
Organisational context		X	X	X
Leadership and Commitment		X	X	X
Management System Support			X	X
Planning and Resources		X		X
Human Resource Management			X	X
Control of Documents and Records		X		X
Objectives / Performance Monitoring & Measurement		X		X
Management Review		X	X	X
Supply Chain				X
Internal Audits		X	X	X

Actions / Non-Conformity / Incidents / Complaints	X	X	X
Risk Management / Prevention		X	X
Legal and Other Requirements			X
Improvement	X	X	X

Certificate Number - PM 741035

Location reference - 0047358928-001

		Audit1
Business area/Location	Date (mm/yy):	03/21
	Duration (days):	7.5
Scope and Policy		X
Organisational context		X
Leadership and Commitment		X
Management System Support		X
Planning and Resources		X
Human Resource Management		X
Control of Documents and Records		X
Objectives / Performance Monitoring & Measurement		X
Management Review		X
Supply Chain		X
Internal Audits		X
Actions / Non-Conformity / Incidents / Complaints		X
Risk Management / Prevention		X
Legal and Other Requirements		X
Improvement		X

Expected outcomes for accredited certification.

What accredited management system certification means?

To achieve an organization's objectives related to the Expected Outcomes intended by the management systems standard, the accredited management system certification is expected to provide confidence that the organization has a management system that conforms to the applicable requirements of the specific ISO standard.

In particular, it is to be expected that the organization

- has a system which is appropriate for its organizational context and certification scope, a defined policy appropriate for the intent of the specific management system standard and to the nature, scale and impacts of its activities, products and services over their lifecycles, is addressing risks and opportunities associated with its context and objectives;
- analyses and understands customer needs and expectations, as well as the relevant statutory and regulatory requirements related to its products, processes and services;
- ensures that product, process and service characteristics have been specified in order to meet customer and applicable statutory/regulatory requirements;
- has determined and is managing the processes needed to achieve the Expected Outcomes intended by the management system standard;
- has ensured the availability of resources necessary to support the operation and monitoring of these products, processes and services;
- monitors and controls the defined product process and service characteristics;
- aims to prevent nonconformities, and has systematic improvement processes in place including the addressing of complaints from interested parties;
- has implemented an effective internal audit and management review process;
- is monitoring, measuring, analysing, evaluating and improving the effectiveness of its management system and has implemented processes for communicating internally, as well as responding to and communicating with interested external parties.

What accredited management systems certification does not mean?

It is important to recognize that management system standards define requirements for an organization's management system, and not the specific performance criteria that are to be achieved (such as product or service standards, environmental performance criteria etc).

Accredited management systems certification should provide confidence in the organization's ability to meet its objectives related to the intent of the management system standard. A management systems audit is not a full legal compliance audit, and does not necessarily ensure ethical behaviour or that the organization will always achieve 100% conformity and legal compliance, though this should of course be a permanent goal.

Within its scope of certification, accredited management systems certification does not imply or ensure, for example:

- that the organization is providing a superior product and service, or
- that the organization's product and service itself is certified as meeting the requirements of an ISO (or any other) standard or specification.

Definitions of findings:

Nonconformity:

Non-fulfilment of a requirement.

Major nonconformity:

Nonconformity that affects the capability of the management system to achieve the intended results.

Nonconformities could be classified as major in the following circumstances:

- If there is a significant doubt that effective process control is in place, or that products or services will meet specified requirements;
- A number of minor nonconformities associated with the same requirement or issue could demonstrate a systemic failure and thus constitute a major nonconformity.

Minor nonconformity:

Nonconformity that does not affect the capability of the management system to achieve the intended results.

Opportunity for improvement:

It is a statement of fact made by an assessor during an assessment, and substantiated by objective evidence, referring to a weakness or potential deficiency in a management system which if not improved may lead to nonconformity in the future. We may provide generic information about industrial best practices but no specific solution shall be provided as a part of an opportunity for improvement.

Observation:

It is ONLY applicable for those schemes which prohibit the certification body to issue an opportunity for improvement.

It is a statement of fact made by the assessor referring to a weakness or potential deficiency in a management system which, if not improved, may lead to a nonconformity in the future.

How to contact BSI

Visit the BSI Connect Portal, our web-based self-service tool to access all your BSI assessment and testing data at a time that's convenient to you. View future audit schedules, submit your corrective action plans and download your reports and Mark of Trust logos to promote your achievement. Plus, you can benchmark your performance using our dashboards to help with your continual improvement journey.

Should you wish to speak with BSI in relation to your certification, please contact your local BSI office – contact details available from the BSI website: <https://www.bsigroup.com/en-US/contact-us/>

Notes

This report and related documents are prepared for and only for BSI's client and for no other purpose. As such, BSI does not accept or assume any responsibility (legal or otherwise) or accept any liability for or in connection with any other purpose for which the Report may be used, or to any other person to whom the Report is shown or in to whose hands it may come, and no other persons shall be entitled to rely on the Report. If you wish to distribute copies of this report external to your organization, then all pages must be included.

BSI, its staff and agents shall keep confidential all information relating to your organization and shall not disclose any such information to any third party, except that in the public domain or required by law or relevant accreditation bodies. BSI staff, agents and accreditation bodies have signed individual confidentiality undertakings and will only receive confidential information on a 'need to know' basis.

This audit was conducted through document reviews, interviews and observation of activities. The audit method used was based on sampling the organization's activities and it was aimed to evaluate the fulfilment of the audited requirements of the relevant management system standard or other normative document and confirm the conformity and effectiveness of the management system and its continued relevance and applicability for the scope of certification.

As this audit was based on a sample of the organization's activities, the findings reported do not imply to include all issues within the system.

Regulatory compliance

BSI conditions of contract for this visit require that BSI be informed of all relevant regulatory noncompliance or incidents that require notification to any regulatory authority. Acceptance of this report by the client signifies that all such issues have been disclosed as part of the assessment process and agreement that any such non-compliance or incidents occurring after this visit will be notified to the BSI client manager as soon as practical after the event.

Microsoft Corporation
One Microsoft Way
Redmond, WA 98052-6399

Tel (425) 882-8080
Fax (425) 936-7329
[Http://www.microsoft.com](http://www.microsoft.com)



April 5th, 2022

To: Clients of Office 365

Re: Additional communication related to the Report on Controls Placed in Operation as of October 1st, 2021 (the "SSAE 18 Report" and "AT 101")

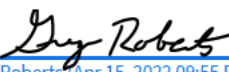
To whom it may concern,

Microsoft recognizes the need to maintain an appropriate internal control environment and report on the effectiveness of, as well as material changes to, its system of internal control. This letter confirms that based on our records, and to the best of our knowledge, for the period October 1st, 2021, through March 31st, 2022, we are not aware of any material changes to the system of internal control provided by Microsoft, that we believe would impact the conclusions reached in the SOC 1 type 2 and SOC 2 type 2 reports.

This letter is not intended to be a substitute for the SOC 1 type 2 and SOC 2 type 2 reports, or to provide you with a certification of Microsoft's internal control, or to suggest to you that Microsoft has performed a separate evaluation of its controls for the purposes of producing this letter. So, to conclude upon the design effectiveness of internal controls at Microsoft, you also should request and read the SOC 1 type 2 and SOC 2 type 2 reports.

These communications, also known as bridge letters, are published quarterly, upon the completion of the quarter.

Sincerely,

X 
Greg Roberts (Apr 15, 2022 09:55 PDT)

Greg Roberts
Principal Group Program Manager, Office 365...



NOTICE: You and your company have obtained access to this report on the description of the system of Microsoft Corporation – Office 365 (this “SOC 1 Report”) by accepting the terms of the Access Agreement that was attached to this SOC 1 Report and acknowledging that your company is a prospective customer of Microsoft Corporation – Office 365 (“Office 365”). The terms of the Access Agreement include, among other things, an agreement by you and your company not to further disclose, distribute, quote, or reference this SOC 1 Report and an agreement to release and indemnify Deloitte & Touche LLP (“Deloitte & Touche”), its subsidiaries and its subcontractors, and their respective personnel. By reading this SOC 1 Report, you reconfirm your agreement to the terms of such Access Agreement. If you are not a prospective customer of Office 365 then you are not authorized to possess, read, or have access to this SOC 1 Report and should immediately return this SOC 1 Report to Office 365.

This SOC 1 Report is intended only to be used by Office 365’s existing clients during the period 10/1/2020, through 9/30/2021, and their external auditors (i.e., “user entities”) during the period 10/1/2020, through 9/30/2021, and the “user auditors,” respectively, as stated in the independent service auditors’ report contained in this SOC 1 Report and defined in the American Institute of Certified Public Accountants’ Statement on Standards for Attestation Engagements No. 18 and International Auditing and Assurance Standards Board’s International Standard on Assurance Engagements (ISAE) 3402 (ISAE 3402) (“Permitted Users”). Deloitte & Touche, the entity that issued the independent service auditors’ report contained in this SOC 1 Report, its subsidiaries and subcontractors, and their respective personnel shall have no liability, duties, responsibilities or other obligations to any entity who may obtain this SOC 1 Report who is not a Permitted User, including, without limitation, any entity who obtains this SOC 1 Report in contemplation of contracting for services with Office 365.

Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have no responsibility for the description of the system of Office 365, including the control objectives and the controls. Nor do Deloitte & Touche, its subsidiaries and subcontractors, and their respective personnel have any obligation to advise or consult with any entity regarding their access to this SOC 1 Report. Any use of this SOC 1 Report by a party other than a Permitted User (“Other Third Party”) is at the sole and exclusive risk of such Other Third Party and such Other Third Party cannot and shall not rely on this SOC 1 Report. This SOC 1 Report is not to be further disclosed, distributed, quoted, or referenced to any third party or included or incorporated by reference in any other document, including any securities filings.



Microsoft Corporation— Microsoft Office 365

System and Organization Controls Report

October 1, 2020, through September 30, 2021

Deloitte.

This report, including the description of tests of controls and results thereof in Section IV, is intended solely for the information and use of management of the Service Organization, user entities of the Service Organization's system related to the in-scope features during some or all of the period October 1, 2020, to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Table of Contents

Section I: Independent Service Auditor's Report	1
Section II: Management's Assertion	5
Section III: Description of the System	8
Section IV: Information Provided by Independent Service Auditor, Except for Control Objectives and Control Activities	34
Section V: Supplemental Information Provided by Microsoft	53

Executive Summary

Microsoft Corporation—Office 365

Scope	Microsoft Office 365 (O365) including Microsoft Office 365 with International Traffic in Arms Regulations (ITAR) ¹ Support
Period of Examination	October 1, 2020, through September 30, 2021
Location(s)	Redmond, WA
Subservice Providers	Yes – <ul style="list-style-type: none">• Microsoft Azure (“Azure”) including Microsoft Datacenters
Opinion Result	Unqualified
Testing Exceptions	4
Complementary User-Entity Controls	Yes – See Page 29
Complementary Subservice Organization Controls	Yes – See Page 31

¹ This report is a description of the “Microsoft Office 365 with ITAR Support system” (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

Section I:

Independent Service Auditor's Report

Microsoft Corporation
Redmond, Washington, 98052

Scope

We have examined the description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") related to its Office 365, including Office 365 with ITAR² Support, online services ("O365") for processing user entities' transactions throughout the period October 1, 2020, to September 30, 2021 (the "Description"), and the suitability of the design and operating effectiveness of controls included in the Description to achieve the related control objectives also included in the Description, based on the criteria identified in **Section II** (the "Assertion"). The controls and control objectives included in the Description are those that management of Microsoft believes are likely to be relevant to user entities' internal control over financial reporting and the Description does not include those aspects of the system of Microsoft that are not likely to be relevant to user entities' internal control over financial reporting.

The information included in **Section V**, *Supplemental Information provided by Microsoft*, is presented by management of the Service Organization to provide additional information and is not a part of the Service Organization's Description of its system made available to user entities during the period October 1, 2020, to September 30, 2021. Information about the Service Organization's supplemental information in **Section V** has not been subjected to the procedures applied in the examination of the Description and of the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description of the system and, accordingly, we express no opinion on it.

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage services. The Description in **Section III** includes only the controls and related control objectives of the Service Organization and excludes the control objectives and related controls of the subservice organization. The Description also indicates that certain control objectives specified by the Service Organization can be achieved only if complementary subservice organization controls ("CSOCs") assumed in the design of the Service Organization's controls are suitably designed and operating effectively, along with the related controls at the Service Organization. Our examination did not extend to controls of the subservice organization or their functions, and we have not evaluated the suitability of the design or operating effectiveness of such CSOCs.

The Description indicates that certain control objectives specified in the Description can be achieved only if complementary user entity controls contemplated in the design of the Service Organization's controls are suitably designed and operating effectively, along with related controls at the Service Organization. Our examination did

² This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

In **Section II**, the Service Organization has provided an assertion about the fairness of the presentation of the Description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description. The Service Organization is responsible for preparing the Description and its Assertion, including the completeness, accuracy, and method of presentation of the Description and the Assertion, providing the services covered by the Description, specifying the control objectives and stating them in the Description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the Description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the Description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the Description, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants ("AICPA") and International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's Assertion, the Description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the Description throughout the period October 1, 2020, to September 30, 2021. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves:

- Performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion.
- Assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- Testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- Evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA and accordingly maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their

nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the Description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in **Section IV** of the report.

Opinion

In our opinion, in all material respects, based on the criteria described in the Service Organization's Assertion in **Section II** of the report:

- a. The Description fairly presents the system related to O365 made available to user entities of the system that was designed and implemented throughout the period October 1, 2020, to September 30, 2021.
- b. The controls related to the control objectives stated in the Description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period October 1, 2020, to September 30, 2021, and subservice organization and user entities applied the complementary controls assumed in the design of the Service Organization's controls throughout the period October 1, 2020, to September 30, 2021.
- c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the Description were achieved, throughout the period October 1, 2020, to September 30, 2021, if complementary subservice organization controls and complementary user entity controls assumed in the design of the Service Organization's controls operated effectively throughout the period October 1, 2020, to September 30, 2021.

Restricted Use

This report, including the description of tests of controls and results in **Section IV** is intended solely for the information and use of management of the Service Organization, user entities of the Service Organization's system related to O365 during some or all of the period October 1, 2020, to September 30, 2021, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

Deloitte & Touche LLP

February 14, 2022

Section II: Management's Assertion

Microsoft Corporation's Assertion

We have prepared the description of Microsoft Corporation (the "Service Organization" or "Microsoft") related to its Office 365, including Office 365 with International Traffic in Arms Regulations (ITAR)³ Support, online services ("O365") for user entities during some or all of the period October 1, 2020, through September 30, 2021 (description), and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements.

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage services. The description includes only the control objectives and related controls of Microsoft and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by Microsoft can be achieved only if complementary subservice organization controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with the related controls at Microsoft. The description does not extend to controls of the subservice organizations.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of Microsoft's controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

Description Criteria

We confirm, to the best of our knowledge and belief, that:

1. The description fairly presents the O365 system made available to user entities of the system during some or throughout the period October 1, 2020, to September 30, 2021, for processing their transactions. The criteria we used in making this assertion were that the description:
 - a. Presents how the system made available to user entities was designed and implemented to process relevant transactions, including, if applicable:
 - i. The types of services provided including, as appropriate, the classes of transactions processed.
 - ii. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.
 - iii. The information used in the performance of procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect

³ This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

information and how information is transferred to the reports and other information prepared for user entities.

- iv. How the system captures and addresses significant events and conditions.
 - v. The process used to prepare reports or other information provided to user entities of the system.
 - vi. Services performed by a subservice organization, if any, including whether the carve-out method or the inclusive method has been used in relation to them.
 - vii. The specified control objectives and controls designed to achieve those objectives, including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.
 - viii. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.
- b. The description includes relevant details of changes to Microsoft's system during the period covered by the description when the description covers a period of time.
 - c. The description does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the system that each individual user entity of the system and its auditor may consider important in its own particular environment.
2. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period October 1, 2020, to September 30, 2021, to achieve those control objectives provided that subservice organizations and user entities applied the controls contemplated in the design of Microsoft's controls. The criteria we used in making this assertion were that:
- a. The risks that threaten the achievement of the control objectives stated in the description have been identified by Microsoft.
 - b. Controls identified in our description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in our description from being achieved.
 - c. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Section III:

Description of the System

Overview of Operations

Business Description

Microsoft Corporation's ("Microsoft") Office 365 ("O365") service is a subscription-based business software service hosted by Microsoft and sold directly, or with partners, to various customers worldwide. O365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations.

Customers subscribe to a standard set of features and services which are hosted in a shared, multi-tenant environment. This includes the Government Community Cloud, an Office 365 offering designed for US government customers. Also included is the Government Community Cloud High and Department of Defense offering, in which customers subscribe to a standard set of features hosted in a multi-tenant environment designed for the US Federal government, defense industry, aerospace industry, and government contractors to provide United States International Traffic in Arms Regulations (ITAR) support and meet Defense Information Systems Agency requirements.

O365 is physically hosted in Microsoft-managed datacenters. Microsoft Datacenters is an organization within Microsoft that provides hosting and network support solutions for the O365 environment. Microsoft Azure ("Azure") is an organization within Microsoft that provides supporting services for the O365 applications including authentication, virtual server hosting, and system data storage and protection. Microsoft Datacenters is managed and run by Azure and both services are treated as one subservice organization (Azure) but will be referred to separately in this report to clarify which part of the Azure organization is responsible for the different services. Both services are not within the scope of this report.

The following services are provided to all O365 customers:

- Email access and productivity tools
- Team communication and collaboration
- Document and other file storage
- Documents viewed and edited in a Web browser

O365 streamlines workflow for customers by providing them with added security, increased email accessibility, and easy team collaboration by providing hosted messaging and collaboration solutions.

Additionally, O365 is part of the Microsoft Cloud for Financial Services offering. Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft's partners and customers to extend the value of the platform with additional solutions to address the financial industry's most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value. Microsoft Cloud for Financial Services and its capabilities (Unified Customer Profile, Customer Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Azure, Microsoft Dynamics 365, Microsoft Power Platform are not part of the scope of this report.

Applicability of the Report

This report has been prepared to provide information on O365's internal controls that may be relevant to the requirements of its customers and affect the processing of user entities' transactions. The detail herein is intended to meet the common requirements of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. Furthermore, detail is limited to the controls in operation over the system as defined in the O365 scope boundary described below. The authorized users of the system supporting the internal controls are limited to O365 personnel. This report covers the software offerings described in the sections below.

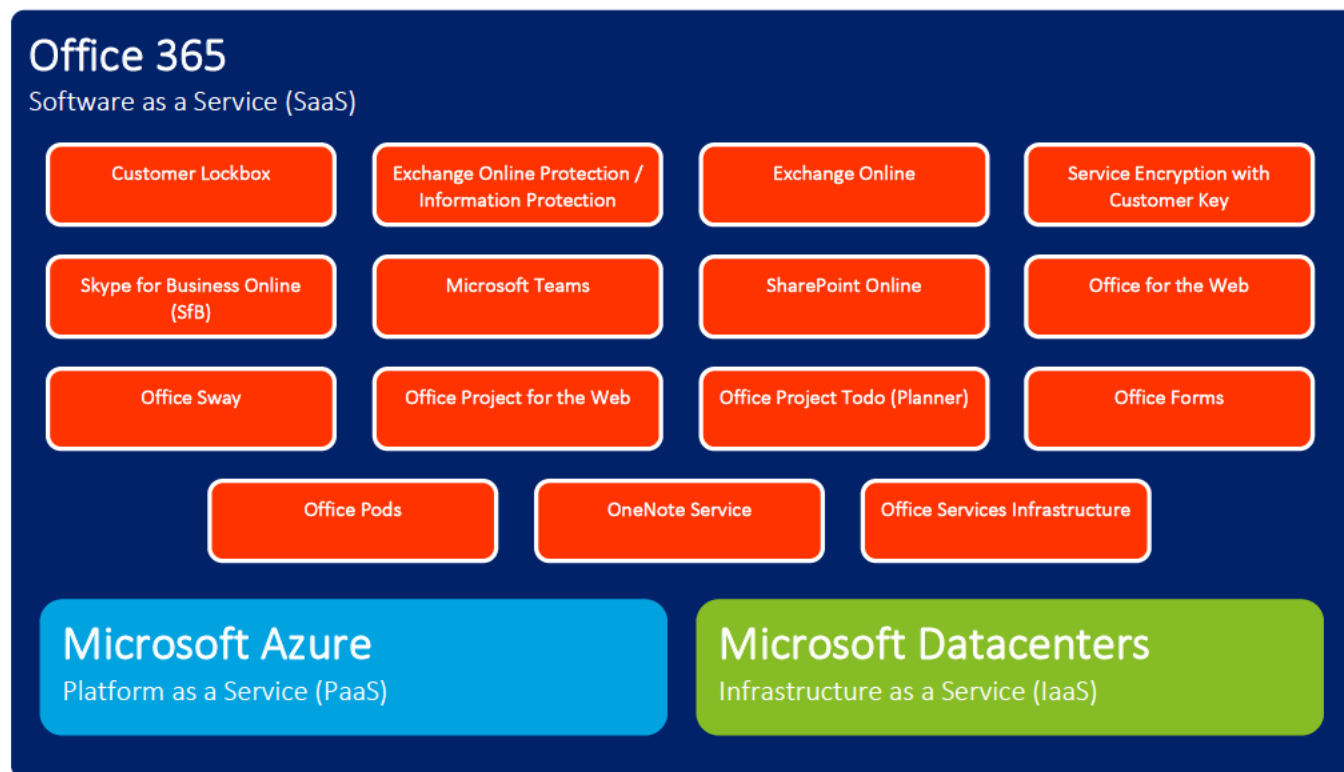
Infrastructure

All O365 services are hosted on a combination of the following subservice organizations within Microsoft: Microsoft Datacenters Infrastructure as a Service (IaaS) and Azure's IaaS and Platform as a Service (PaaS).

For Microsoft Datacenters hosting, the physical servers are owned by O365, the operating system (OS) and software are managed by O365, and network layer and network layer protections are implemented by Microsoft Datacenters. O365 manages the configuration of the network layer/protection in coordination with Microsoft Datacenters.

For Azure's IaaS hosting, O365 is responsible for the OS and database management. For Azure PaaS hosting, O365 is responsible for limited configuration of the OS while Azure is responsible for database and storage setup and maintenance, and overall OS setup and protections. Network layer protections are implemented by Azure for both IaaS and PaaS and are managed in coordination with Azure. Additionally, Azure manages the gateways for remote access into the O365 networks.

In both cases, Microsoft Datacenters is responsible for physical and environmental security. In addition, Azure PaaS provides customer authentication and rights management services through Azure Active Directory (AAD). The controls managed by Microsoft Datacenters and Azure are not in the scope of this report.



Software

O365 includes the following SaaS offerings:

- Customer Lockbox – An access control technology designed to provide customer control and transparency over access to customer content.
- Exchange Online Protection (EOP) – A service providing security features, such as antivirus, antimalware, and antispam filtering for Exchange.
- Information Protection (IP) – A service providing security features, such as antivirus, antimalware, and antispam filtering for Exchange. IP includes the following subservices: Adv eDiscovery, Compliance Manager and STP, Data Insights V2, Exact Data Match, Import service, Insider Risk Management, ML Inference, and O365 Auditing.
- Exchange Online (EXO) – An email service.
- Service Encryption with Customer Key – A service providing customers with two application-level encryption options for customer content at rest within the Exchange and SharePoint environments: Service Encryption with Microsoft-owned encryption keys and Service Encryption with customer-owned encryption keys (“Customer Keys”).
- Skype for Business Online (SfB) – A communication service that offers collaboration capabilities via instant messaging, audio and video calling, online meetings, and web conferencing.
- Microsoft Teams – A communication service that offers a threaded persistent chat experience that builds on O365’s group infrastructure, global scale, enterprise grade security, and graph driven intelligence. Microsoft Teams is also referred to as Azure Communication Service (ACS).
- SharePoint Online (SPO) – A solution for creating websites to share documents and information with colleagues and customers. This information and documentation repository includes OneDrive, Delve, Access Online, and Project Online.
- Office for the Web (WAC) (formally Office Online) – Enables users to access, view, and edit documents online via a web browser.
- Office Sway – Digital storytelling app for creating interactive reports, presentations, personal stories, and more.
- Office Project Todo (Planner) – Provides a visual way to organize teamwork and simplified task management.
- Office Forms – Create surveys, quizzes, and polls with real-time results, built-in response analytics, and export to Excel.
- Office PODS – PowerPoint Online Document Service (PODS) streams images representing slides or pages of an Office file to SharePoint on-demand.
- OneNote Service – Provides an Application Programming Interface to OneNote Notebooks on SharePoint.
- Office Services Infrastructure (OSI) – A platform for backend applications including deployment, hosting, and monitoring infrastructure applications.

O365 uses the following software to support the above offerings:

- Microsoft 365 (M365) Remote Access – A set of servers providing remote access to O365 service production environments via authorized two-factor authentication and encryption. This service was deprecated during the audit period and replaced with Azure Gateway, which is managed by the Azure subservice organization.

- Identity Manager (IDM) – An access management service providing an integrated and broad solution for managing O365 user identities and associated credentials for all O365 services (with the exception Microsoft Teams, which leverages MyAccess).
- Intelligent Conversation and Communications Cloud (IC3) – A supporting service for the SfB and Microsoft Teams services supporting first-party real-time conversation products including audio and video calling, meetings, and chat services.

In addition to the product software, the following utilities are used by the service teams to execute controls relevant to the O365 system but are not directly covered in this report:

- Employee Cloud Screening (ECS) – An SAP add-on used by Microsoft Human Resources that hosts employee background check information that synchronizes with IDM databases to limit user access to eligibilities based on background check status.
- Substrate, Office Substrate Pulse (OSP) – A platform and system tools for centrally managing and hosting applications and services that are used internally by O365 and by customers.
- Qualys – Scanning systems used to identify and resolve security vulnerabilities within the O365 environment.
- CorpFIM/IDWeb, MyAccess, and Torus – O365 user management tools used to grant temporary user access time-bound permissions and access to sensitive systems, including access to customer content.
- Remote Desktop Services – The accepted method for Microsoft personnel to gain logical access to the O365 environment remotely using Azure Gateway managed Remote Desktop Gateways (RDGs).
- Griffin/Office Supporting Infrastructure, O365SuiteUX Environments and Release Dashboard, PilotFish, and Azure DevOps – Change management tools used by service and support teams to track and deploy code changes to production environments.
- Aria, Avocado, Geneva, Incident Manager (IcM), Jarvis, and Heat Map – Dashboards and alerting systems that monitor the capacity and availability of the servers and services based on pre-determined capacity and availability thresholds. In the event of a breach of a capacity or availability threshold, automated alerts are generated and communicated to the service team's respective on-call engineer for tracking and remediation. Additionally, they provide a visual representation of major/minor system releases across various stages including preproduction, testing, and production.

People

O365 personnel are organized into service teams that develop and maintain the application and the support teams that provide supporting services for system operations.

Each service and support team for O365 has defined responsibilities and accountabilities to manage security, availability, processing integrity, and confidentiality of the applications. The teams include the following groups:

- Access Security – Personnel that maintain Active Directory (AD) services, authentication rules and user access.
- Change Management – Development, testing, and project management teams tasked with developing and maintaining the O365 applications and supporting services.
- Backups and Replication – Personnel for configuring and monitoring the replication and backup of specified internal and customer content.
- Security and Availability Monitoring – Personnel that monitor the incidents that affect the security and availability of O365 applications and supporting services.

In addition to service teams, centralized support teams provide specialized functions for the services, including the following:

- Enterprise Business Continuity Management (EBCM) – A single resource to assist O365 teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.
- O365 Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.
- Governance, Risk, and Compliance (GRC) – Identifies, documents, and advises teams in implementing controls to maintain O365’s availability and security commitments to its customers.
- Office Trustworthy Computing (OTwC) – Develops and enforces the Secure Development Lifecycle process for O365 applications and support services.
- Identity Management (also known as Access Control team) – Operates the IDM tool to provide access control automation for all teams (excluding Microsoft Teams).
- Microsoft Information Technology (MSIT) – Provides the access control and authentication mechanism for Microsoft Teams via MyAccess.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and AAD.
- Microsoft 365 Remote Access – Provides internal users remote access control and authentication to the O365 environment.
- Security Incident Response (SIR) – An internally focused resource that provides detection and analysis as well as containment, eradication and remediation for severe security incidents that may affect the O365 services.

Procedures

O365 adheres to Microsoft Corporation’s Security Policy, which is owned by the Information Risk Management Council (IRMC), comprising business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) for Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- | | |
|---------------------------------------|---|
| • Human resources security | • Systems acquisition, development, and maintenance |
| • Asset management | • Supplier relationships |
| • Access control | • Information security incident management |
| • Cryptography | • Business continuity management |
| • Physical and environmental security | • Compliance |
| • Operations security | |
| • Communications security | |

O365 uses National Institute of Standards and Technology (NIST) standard 800-53 for baseline control procedures, which are documented in the O365 control framework. Control measures above and beyond NIST 800-53 are included to address the full range of Microsoft contractual and regulatory commitments. The framework covers the following areas:

- Access Control
- Accountability, Audit, and Risk
- Authority and Purpose
- Awareness and Training
- Configuration Management
- Contingency Planning
- Data Minimization and Retention
- Data Portability
- Data Quality and Integrity
- Geographic Boundaries
- Identification and Authentication
- Incident Response
- Individual Participation and Redress
- Maintenance
- Media Protection
- Personnel Security
- Physical Access
- Program Management
- Risk Assessment
- Security
- Security Assessment
- Security Planning
- System Access
- System and Communication Security
- System and Information Integrity
- System and Services Acquisition
- Use Limitation

In addition to the above procedures, manual and automated control activities are described in the section “Description of Control Activities” below.

Data

O365 customer content is maintained in Azure and SQL server databases, which are hosted on a defined Windows AD domain. Each service and support teams are responsible for managing the security, availability, processing integrity, and confidentiality of the data in Azure or on the database servers. The table below details the data classifications for this report and the O365 environment.

Data Classification	Definition
Access Control Data	Data used to manage access to administrative roles or sensitive functions.
Customer Content	Content directly created by users. Content is not viewed by Microsoft personnel unless required to resolve a ticketed service problem.
End User Identifiable Information (EUII)	Data unique to a user, or generated from a user’s use of the service: <ul style="list-style-type: none"> – Linkable to an individual user – Does not contain Customer Content
Organization Identifiable Information (OII)	Data that can be used to identify a tenant (generally configuration or usage data): <ul style="list-style-type: none"> – Not linkable to an individual user – Does not contain Customer Content
System Metadata	Data generated while running the service, which is not linkable to an individual user or tenant and does not contain Customer Content, EUII, OII, or Account Data.
Account Data	Administrator Data Payment Data Support Data

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with a board of directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

- To establish and preserve management accountability to Microsoft's owners by distributing rights and responsibilities among Microsoft Board members, managers, and shareholders.
- To provide a structure through which management and the board set and attain objectives and monitor performance.
- To strengthen and safeguard a culture of business integrity and responsible business practices.
- To encourage the efficient use of resources and to require accountability for the stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft website, www.microsoft.com.

Microsoft's Standards of Business Conduct

Microsoft's Standards of Business Conduct ("SBC") reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full consideration of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") and NASDAQ listing requirements related to codes of conduct.

Further information about Microsoft's SBC is available on the Microsoft website, www.microsoft.com.

Training and Accountability

O365 leverages the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and to act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees (including O365), contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course upon being hired and again on an annual basis thereafter. In addition, employees are required to participate in mandatory security and compliance trainings periodically in order to design, build, and operate secure cloud services.

Microsoft O365 staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and applicable supporting standards. Individuals not employed by O365, but allowed to access, manage, or process information assets of O365 are also accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and associated standards.

Commitment to Competence

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make appropriate hiring decisions.

Microsoft employees create individual accountabilities that align with those of their managers, organizations, and Microsoft, and are supported by customer-centric actions and measures so that everyone is working toward the same overarching vision. Accountabilities are established when an employee is hired and then updated throughout the year according to business circumstances.

Managers work with their employees to analyze progress against accountabilities and to adjust accountabilities, if needed, several times throughout the year. Managers evaluate individual contributions to teams, the business, or customer impact, taking into consideration contributions aimed at creating a high performing team and the demonstration of competencies relevant to the role.

Office of Legal Compliance — Board of Directors and Senior Leadership

The Office of Legal Compliance (OLC) designs and provides reports to the board of directors on compliance matters. The OLC also organizes annual meetings with the Senior Leadership team for its compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) function that reports directly to the Audit Committee (AC) of the board of directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. The responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

Audit Committee

The AC charter and responsibilities are on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar set out in the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for Identification of Risk

IA, the Financial Compliance group, and the Finance Risk group perform formal risk identification processes each year. These assessments cover risks over financial reporting, fraud, and compliance with laws.

Internal audit — Fraud Risks

IA and the Financial Integrity Unit (FIU) look for fraud risk. The FIU performs procedures for the detection, investigation, and prevention of financial fraud affecting Microsoft worldwide. Fraud and abuse that is uncovered is reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), HR, Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA and other groups within the company perform periodic risk assessments. These assessments are reviewed by senior management.

IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business processes, and systems controls. Control failures are also analyzed to determine whether they give rise to additional risks.

Annual Risk Assessment

The annual risk assessment process is established to monitor, manage, and mitigate specific business risks related to security for customers and partners. Led by the Risk Management office, Microsoft follows an established approach to risk management and conducts an annual global risk assessment beginning in the first quarter of each fiscal year. The purpose of the annual risk assessment is to identify and prioritize each division's specific strategic and operational risks based on impact, likelihood, and management control. Additionally, accountability is established for each risk and mitigation decisions are made at the Corporate Vice President level with transparency across the leadership team.

OLC/IA/Risk Management — Risk Responsibility

The responsibility for risk is distributed throughout the organization based on each individual group's services. OLC, IA, and the Risk Management Group work together to represent enterprise risk management. Through quarterly and year-end reviews, the Chief Financial Officer (CFO) and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Information and Communication

Internal Communication

Responsibilities concerning internal control are communicated broadly, which includes Monthly Controller calls, All Hands Meetings run by the CFO, and update conference calls held by the Financial Compliance Group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are set out in the SBC for which a mandatory training has been established for all employees. Additionally, compliance managers meet with control owners to make sure they understand the controls for which they are accountable and update the controls based on changes in the business environment.

Office of the CFO — Communications External to the Company

CFO communications outside the company occur throughout the year and, where applicable, these external communications include discussions of the company's attitude toward sound internal controls. The Office of the CFO is responsible for several communications outside of Microsoft including quarterly earnings releases, financial analyst meetings, customer visits, outside conferences, and external publications.

Monitoring

OLC — Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24 hours per day and 7 days per week through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance. Employees are instructed that it is their duty to promptly report concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their manager, senior leadership, CELA contact, HR contact, or the Compliance Office.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively analyzing whether the objectives of management are adequately performed, as well as facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Monitoring of Subservice Organizations

O365 uses Microsoft Azure including the Microsoft Datacenters service, which manages datacenters, IaaS, and PaaS supporting services for the O365 applications including hosting of servers, network support, authentication, virtual server hosting and system data storage. Note that O365 considers Azure and Microsoft Datacenters as two separate organizations within this report and are defined as such.

The O365 GRC team is responsible for identifying dependencies of each service and monitoring the subservices implementation of agreed-upon security, availability, processing integrity, and confidentiality controls.

Dependencies are documented in Inter-Service Agreements. Monitoring includes, but is not limited to, the review of third-party service auditor reports and discussions with subservice organization management.

A brief overview of the subservice organizations used by Microsoft O365 is below.

Organization	Brief Description
Microsoft Azure	Microsoft Azure's cloud PaaS offerings are used by O365 to host production data and handle logical access and change management controls for O365.
Microsoft Datacenters	Microsoft Datacenter's IaaS offerings are used by O365 to host physical and virtual servers and system data storage. Microsoft Datacenters also handles physical and environmental security controls for O365.

Description of Control Activities

Logical Access	
Control Objective 1	Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
Change Management	
Control Objective 2	Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.
Data Backup and Restoration	
Control Objective 3	Data replication or backup controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.
Monitoring and Incident Management	
Control Objective 4	The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.
Network Services	
Control Objective 5	Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks.
Customer Lockbox	
Control Objective 6	Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

Logical Access

Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.

Control Objective 6: Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

Overview

Background Checks

Backgrounds checks are required for all US based full-time employees and vendors before access is granted to certain eligibilities within each workstream. US background checks are renewed every two years. Microsoft has rolled out an international screening program, which requires background screening and renewals for all new Full Time Employee ("FTE") and vendor personnel in forty-four countries, as permitted by the laws of each country.

Microsoft full-time employees request background checks, when necessary, through the OSP employee portal. A notification is sent to the requesting employee's manager for approval. If approved, a notification email is sent to Microsoft HR to process a background check for the requesting employee. When the background check is complete, HR enters the results into ECS.

For vendors and contractors, vendor companies are responsible for completing a valid background check for each contracted vendor. Once completed, Microsoft receives an attestation letter from the vendor company confirming the completion and pass status of the vendor's background check. Once the background check validation is received, Microsoft enters relevant information into ECS. Background check information for FTEs and vendors is pushed from ECS to an IDM database, after which the IDM tool checks for employee background check information before access to O365 cloud environments can be requested by the employee. Full and incremental sync jobs run to keep the data used by the IDM tool current.

Workload administrators configure requirements, including background check, for eligibilities within each workstream. If no background check is on file, or if a background check has expired, the user receives an error indicating that the employee does not have required background check, thus preventing the employee or vendor from obtaining those eligibilities.

Identity Access Management

Microsoft O365 owns and manages tools that regulate access to O365 production environments. Most service teams use the IDM access management service to limit access to authorized users. The service, managed by the Access Control team, allows each of the other service teams to manage their respective AD clusters for their respective environment. Several backend processes synchronize with other internal Microsoft tools, such as Microsoft HR department systems, to check that user information (e.g., employment status, manager, cost center, background check information) meets predefined requirements. Users who meet predefined criteria can request access to certain eligibilities, and access is only granted after approval.

Some access is regulated outside the IDM service via other tools and processes; however, the functionality and processes are the same. These tools include IDWeb and MyAccess.

New User or Modification of User Access

The process to request and approve new access via access management tools is managed through automated workflows configured within the tools. The systems automatically route access requests to the requestor's manager for approval. Users who meet specified requirements (e.g. active user, active manager, applicable cost center, or background check) can request specific access to rights within each environment. User requests trigger

notifications to the user's manager via email of a pending access request requiring manager approval. No access is provisioned within production environments until manager approval is obtained.

There are certain groups, roles, or entitlements that fall outside the automated provisioning processes described above. In each case users must still submit access requests, and each request must be approved before the access is manually provisioned.

External Users (Customer Entities) – When a new customer is added to the O365 service, they are provided with an initial account for system setup. The provisioning of users and deactivation of users is the responsibility of the customer entity.

Termination Access Removal

When individuals leave the company, Microsoft HR updates the terminated employee's details in the HR system, which syncs to access management tools via backend tasks. Access for terminated employees is then removed from respective service production environments. Without the appropriate entitlements, the user cannot access services within the O365 environment.

Periodic User Access Review

Services using the automated access provisioning processes above rely on workflows within the systems to automatically revoke user access based on the following criteria:

- *Inactivity* - After 56 days of inactivity, the user's account is disabled.
- *Manager Change* - When a user's manager and/or cost center has changed, users must re-request access using the same process described above, and the new manager must approve the user's requested access.
- *Group Pre-defined Expiration* - Where applicable, workloads have security groups that have a set expiration period from when an account was granted access to the group.

For manually maintained user access, a manual user access review is performed on a periodic basis to substantiate that access for each user is relevant and in line with job responsibilities. Any needed access alterations identified during the review are addressed in a timely manner.

Just-in-Time Access

Just-in-time (JIT) tools allow individuals to request temporary elevated access privileges on an as-needed basis to limited areas within the respective service team's associated Windows AD environments.

Each tool follows a similar process before granting temporary elevated access to requesting engineers. Automated configurations within each tool notify the submitting user's manager with details of the access requested. If approved, the requesting user is granted access on a temporary basis, and the tool automatically removes the requested access based on built-in functionality within the tool. In certain cases, an engineer may receive a one-time preapproval for access elevations to specific areas within an environment; however, the access is still temporary in duration. Additionally, each elevation is logged and retained by the service team for incident evaluations.

Developer/Operations Model - Developer Access to Production

Using the Access tools described above the service teams have restricted access to appropriate personnel, including the enforcement of segregation between developers and operations personnel.

Select service teams allow developers temporary access to production using the JIT tools and approval processes described above. Developer access is limited to specific areas of the environment for deployment or operations purposes. These limitations are enforced using Torus, a Remote PowerShell tool. Torus allows for the restriction

of access to specific commands that can be run in the service team's environment and requires approvals for each command being requested. The Torus request and approval process is managed by the JIT tools described above. For requests to make changes to production code or data by a developer or operator, an associated service request ticket must be provided and approved by a separate individual.

Authentication

Internal users are authenticated using Remote Desktop Services and must be authenticated using a two-factor authentication mechanism that includes a smartcard with PIN to log into the RDG. After logging in to the RDG, the user must enter his/her production account user ID and password to access production servers. The corporate password requirements are defined and configured in each service teams' and support teams' Windows AD domain. These requirements include password complexity, length, history, and duration. Additionally, internal users can gain temporary access to elevated roles allowing access to customer content via the JIT methods described above. For those services that only use JIT elevations to access the environment with no standing access, there are requirements built into the JIT tools for generating onetime complex passwords for authenticating into these environments.

External Users – Microsoft provides various options to enable the authentication mechanism for end users and O365 customers. Each external entity is responsible for substantiating that the mechanism is configured and operating, as well as enforcing the use of strong passwords.

Customer Lockbox

Customer Lockbox is an access control technology included in O365, designed to provide customer control and transparency over access to customer content hosted in Microsoft datacenters. The service grants Microsoft engineers temporary access to customer content on as-needed basis only as approved by an appropriate tenant authority. The following sections, prefixed with "Customer Lockbox," detail the procedures in place to limit Microsoft access to customer generated content.

Customer Lockbox - Authorization and Notification

Access to customer content for customers utilizing the Customer Lockbox feature is initiated through a Service Request made via Microsoft's customer support. If the Service Request requires access to customer content, the access is requested through the Customer Lockbox tool. Individuals who are approved to access the customer content do so using the RPS tool.

Only Microsoft engineers with appropriate access entitlements within the Exchange environment, can request temporary elevation to the 'AccessToCustomerData' role, which allows access to customer content. The request process is built into Customer Lockbox. If approved by the role owners, Microsoft managers, the request is then routed to a customer contact for additional approval.

Customer Lockbox - Customer Approval

The automated workflows supporting the Customer Lockbox elevation process require that elevation requests are first approved by Microsoft management before being submitted to a tenant administrator. Tenant administrators are assigned and are the responsibility of each customer. If the request is not approved within a specified period of time by both the Microsoft management and the tenant administrator, then the elevation request times out and becomes invalid.

Customer Lockbox - Associated Service Request

Each elevation request made using Customer Lockbox must reference an associated service request number before submission to Microsoft management for approval. Attempts to submit an elevation request without an associated service request number will fail, and the RPS tool will return an error. Service requests are either

submitted by the effected customer or created and communicated to the customer prior to the elevation request.

Customer Lockbox - Office 365 Admin Center

O365 customers can review a history of Customer Lockbox elevation requests within the customer's O365 Admin Center. The history includes relevant information for current and past elevation requests, including the date, service request number, duration of elevation, reason for elevation, and requestor. The logs are kept for a reasonable period of time.

Customer Lockbox - Searchable Audit Logs

Server activity is logged for each Customer Lockbox elevation, and the activity log repository is available to each Customer Lockbox customer. Activity logs show what actions and commands were executed on a server containing customer content by a Microsoft engineer for the time allowed during an elevation requested through Customer Lockbox.

Customer Lockbox - Management Review of Elevations

Microsoft management pulls logs of Customer Lockbox elevations, as well as capacity server administrator elevations, from a data repository and investigates any anomalies. The statistics are reviewed as part of a Monthly Service Review with Microsoft management. For customers who have chosen to use Customer Lockbox, it is the only way to access customer content. Any other access paths are considered malicious access and are not covered by this attestation.

Data Management

Data Segregation

Customer content is stored and processed on a shared database which is logically segregated using program logic and a different customer identifier.

Change Management

Control Objective 2: Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.

Service Infrastructure and Support Systems Change Management

Service- and support-related changes follow an established change management process for the O365 environment. Each change is tracked within identified ticketing systems, which contain information that can be linked to approval and testing details related to the change. These ticketing systems are listed in the Software section above. Appropriate authorizations and approvals needed for the changes being made to these environments are defined in the tickets.

When service teams or customer representatives enter a request for a change to the O365 environment in the change management systems, a representative of the relevant workstream is charged with addressing the change request. If a code modification is required, the addressor will perform a pull request, which replicates the master branch's code and allows the user to perform necessary code modifications without disrupting the live code running in production. Each individual change or addition made to address the change request is subject to a peer review in which another workstream representative reviews and approves the individual code changes. Once a change is peer reviewed and approved, it is checked into a build, along with other changes that are currently in the workstream's deployment process. Each build is subject to security and static analysis testing to test for the presence of security vulnerabilities. Except for in specific scenarios, O365 environment change management processes require 100% testing pass rates prior to moving forward in the deployment process. When a build successfully completes security testing, it is deployed to preproduction environments for integration testing. Builds can be independently deployed to the preproduction environments or multiple builds can be aggregated into a "release," which is subject to integration testing. Code that has successfully completed all testing types is then deployed to the master code repository and is recognized as the newest version of the workstream's source code. There are generally three types of preproduction environments, or "rings," for ring validation integration testing:

- DogFood: The workstream's initial test ring consisting of a subset of Microsoft employees and customers who test changes on Microsoft's behalf.
- MSIT: The MSIT ring allows the release to be subject to testing by all Microsoft employees.
- Slice in Production (SIP): Once the release is successfully integrated into the MSIT ring, it is moved into the SIP environment, which consists of about 5% worldwide customers who have decided to opt in and are able to provide feedback.

Certain types of changes in O365 change management systems are subject to additional review and approval processes dependent on the nature of the change. The four approval levels based on the nature and impact of the change have been included below:

- Auto-approval – A set of preapproved, low-risk standard changes.
- Functional (Peer) Approval – Standard changes with a slightly higher level of risk.
- Change Advisory Board Approval – Changes with the potential for high risk and high impact.
- Emergency Change Advisory Board Approval – A risk that must be remediated timely, such as an out of band security patch.

O365 service teams use a variety of tools to deploy changes to Azure. The ability to deploy code is restricted to appropriate build deployers using a combination of IDM, Torus, and Lockbox permissions.

Security Development Lifecycle

O365 environments follow the standard Microsoft Security Development Lifecycle (SDL) process which includes, at a minimum, risk assessment, testing, approval, and documentation. The SDL process includes security

development requirements, which are intended to reduce the number of security-related bugs that appear in the design, code, and documentation associated with a software release, as well as to detect and remove those bugs as early in the SDL as possible.

Risk assessment and design review occurs in a Change Advisory Board entitled “Office Hours” whose members formally “Approve” or “Deny” any major or significant change prior to implementation. Members include representatives from Compliance, Security, OTwC, and Microsoft Legal teams.

Testing, including code reviews, occurs during the development and build processes. Results of the tests, reviews, and approvals are tracked through ticketing systems used by each team. These ticketing systems are listed in the Software section above.

Data Backup and Restoration

Control Objective 3: Data replication or backup controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.

Data Replication and Data Backup

Data for customer content, applications and support services is replicated for redundancy and disaster recovery purposes. O365 applications and supporting services are generally replicated from the primary content database to a secondary content database within the same primary datacenter. The primary and secondary databases are then replicated across geographically dispersed datacenters. Generally, the data maintained in the primary content database is replicated and accessible in real time via: (1) the primary database; (2) a secondary replication database located in the same primary datacenter with real time data; (3) a secondary disaster recovery server with real time replicated data in a geographically segregated datacenter; or (4) a server with a few minutes lag replication in a geographically dispersed datacenter.

In addition to content replication and geographical redundancy, O365 customer content data is also subject to a periodic Azure Blob Storage backup process. Customer content is generally subject to three backup types, each with a unique cadence:

- Full Backups – Full backups consist of all customer content data on a server or content database, generally occur on a weekly frequency and are maintained for 30 days.
- Differential Backups – Differential backups occur at a daily frequency and consist of any additional data since the last full backup or differential backup, depending on which was the last to occur.
- Transaction-Log Backups (“TLog”) – TLog backups occur every 5 minutes and consist of any additional data added in every 5-minute interval.

As data is accessible for redundancy and disaster recovery purposes for applications and support services through the data replication process described above, data backup is performed on applications containing customer content to meet the SLA requirements.

It should be noted that the replication process described above reflects the processes in place for the SfB, EXO, and SPO systems at an overall level. The supporting service teams perform similar replication processes, such as utilizing an Active-Active (e.g., EOP) replication process, but do not maintain lag copies of data. Azure based services rely on Azure capabilities for geo-redundant replication and storage.

Business Continuity

The majority of O365 service teams participate in the Enterprise Business Continuity Management (EBCM) program that uses a common set of criteria to determine the relevancy and frequency of failover exercises. Teams not yet integrated into the EBCM process perform periodic failover testing. Where relevant, failover exercises are conducted on a regular basis to test applications and related data to verify the accessibility at a secondary disaster recovery location. The frequency of conducting failover exercises, as well as the recovery time objectives (RTOs) for each application and support service, are based on the nature and criticality of the systems. The RTOs are developed as part of the overall O365 Business Continuity and Disaster Recovery Planning. The primary objective of conducting failover exercises is to test whether the RTOs may be met in case of a disaster. Issues identified as part of the failover tests are tracked to ultimate resolution.

Customer Termination

Customer content is retained after termination of O365 subscriptions per agreed upon commitments with the customer in the contract and SLAs. Customers are responsible for the upload/download and management of data stored within the O365 environments related to confidentiality.

Monitoring and Incident Management

Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

Vulnerability and Patch Management

The O365 Security team monitors for known configuration and patching vulnerabilities through automated scans based on Qualys technology. A master server is configured to scan each server within O365 applications and supporting services AD domains to analyze and report known vulnerabilities and patch non-compliance. Each service team reviews the vulnerability scan report from the master server and assesses the criticality of the vulnerabilities and applies patches as applicable.

New vulnerabilities (e.g., those from responsible disclosure programs) are communicated to O365 through the Microsoft Security Response Center. If a patch is developed for the vulnerability, each service team evaluates the relevance of the patch to its environment and applies the patch as applicable.

Security Incident Monitoring

O365 has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and deter security incidents. The O365 incident management technical infrastructure includes monitoring systems for detecting and alerting O365 personnel of security events and incidents. A monitoring agent is installed on each server at the time of server build-out to transfer the security logs to the Security Incident Response (SIR) team, which identifies potential incidents and serves as a central repository for investigations. Incidents posing significant risk to the environment are prioritized for response and mitigation.

Additionally, each service team has on-call personnel covering a 24/7 schedule. If an incident is assigned a high enough severity, applicable contingency plans are invoked. When a contingency plan is invoked, the incident manager on shift works with the O365 Security team to implement the contingency plan.

Server Build-Out Process

O365 has a defined server build-out process to deploy and configure new servers and rebuild existing servers. As part of the server build-out process, each service team performs the following:

- Connect the server to the specified AD domain.
- Install anti-malware agents to get up to date anti-malware signature files and definitions.
- Install a server agent to collect server activities and upload the logs to the SIR team databases for security assessment activities.

After the base server image is applied and the related build-out process is finished, quality assurance reviews are conducted to validate that the server build-out process completed as expected. The quality assurance review follows one of two processes for server build-out compliance:

- Quality assurance checklist/Automated scan:

As part of the build-out process, each server is scanned using an automated tool. This scan produces a log file that details if the applicable build-out steps were followed and completed successfully. In addition to this scan, teams follow a manual checklist to ascertain that some steps have been completed in the build-out process, which includes evaluating the automated scan log file.

- Automated build-out tool:

Application and supporting service teams that leverage an automated build-out and deployment process utilize a scan performed by the deployment tool to substantiate the build had completed successfully. If there is a failure, the tool attempts to redeploy the build until successful.

Certain services leverage Microsoft's Azure PaaS offerings for server build-out and management. Teams who use Azure IaaS with customized server images maintain, update, and test server images as part of the deployment process. Once the server image has been tested, it is provided to Azure for actual deployment.

Network Services

Control objective 5: Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks.

Network Problem Management

Microsoft Datacenters' Global Networking Services (GNS) has designated teams (i.e., Problem Management, Network Escalations, and Network Security) to identify and address security alerts and incidents. GNS is responsible for identifying and analyzing potential problems and issues in the O365 networking environment.

Network Configuration Monitoring

Microsoft Datacenters' GNS team has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. GNS regularly monitors network devices for compliance with technical standards and potentially malicious activity.

Network Change Management

GNS has implemented a formal change management process that requires network changes, including configuration changes, emergency changes, Access Control Lists changes, and new deployments to be documented and authorized prior to implementation. Changes and change approvals are tracked in a ticketing system.

Server/Network Device Remote Access

Microsoft Datacenters provides remote server and network device access to Microsoft Datacenters-managed environments. Access is provided through Microsoft Datacenters-managed Active Directory security groups and follows standard logical access procedures as established by Microsoft Datacenters and GNS.

Control Objectives and Related Control Activities

The control objectives and related control activities are documented in **Section IV** to reduce the redundancy that would result from listing them in this section and repeating them in **Section IV**. The control objectives and related control activities are however an integral part of the description of the system. While listed in **Section IV**, the service organization remains responsible for the representations in the description of controls. These control activities include preventive, detective, and corrective policies and procedures that help O365 identify, decrease, manage, and respond to risk in a timely manner.

Changes During the Examination Period

During the examination period the SfB and Microsoft Teams services started using an internal Microsoft service called IC3. As part of the transition to IC3, the access management processes were brought into scope for the relevant production environments supported by IC3, including the user access review, access provisioning, and access deprovisioning processes.

Complementary User Entity Control Considerations (CUECs)

Microsoft O365 transaction processing and the controls over that processing were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of O365. The following list contains controls that O365 assumes their user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant Control Objective
User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities establish proper controls over the use of system IDs and passwords.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities are responsible for managing their user's password authentication mechanism.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities enforce desired level of encryption for network sessions.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities manage anonymous access to SPO and SfB sessions.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities secure the software and hardware used to access O365.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
User entities are responsible for enabling and maintaining email restoration for EXO.	Control Objective 3: Data replication or backup controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.

Complementary User Entity Controls	Relevant Control Objective
User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.	Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.
When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner.	Control Objective 6: Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

Complementary Subservice Organization Controls

Microsoft controls related to the O365 system detailed in this report cover only a portion of overall internal control for each user entity of O365. It is not feasible for the control objectives related to O365 to be achieved solely by Microsoft. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with O365's controls, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows:

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Control Objective
Platform as a Service (PaaS) logical access	Microsoft Azure	Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.	Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.
Platform as a Service (PaaS) change management	Microsoft Azure	For certain services, Microsoft Azure is responsible for maintaining controls over the deployment of changes to O365 production environments.	Control Objective 2: Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.
Backups and restoration of customer content	Microsoft Azure	For certain services, Microsoft Azure is responsible for maintaining controls over the restoration, backups, and retention of customer content.	Control Objective 3: Data replication or backup controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.
Operating system configurations	Microsoft Azure	For certain services, Microsoft Azure is responsible for maintaining controls over base operating system images, including security configurations and monitors, applied to servers deployed to O365 production environments.	Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant Control Objective
Infrastructure as a Service (IaaS) physical security	Microsoft Datacenters	Microsoft Datacenters is responsible for maintaining controls over physical security of datacenters supporting Azure and O365.	N/A – Physical Security is wholly carved-out to Microsoft Datacenters.

Section IV:

Information Provided by Independent Service Auditor, Except for Control Objectives and Control Activities

Introduction

This report on the description of the system is intended to provide user entities and their auditors with information for their evaluation of the effect of a service organization on a user entity's internal control relating to Microsoft Corporation's ("Microsoft" or the "Service Organization") controls over its Office 365 and Office 365 with International Traffic in Arms Regulations (ITAR) Support systems ("O365") during some or all of the period October 1, 2020, through September 30, 2021.

This section presents the following information provided by Microsoft:

- The control objectives specified by the management of Microsoft.
- The controls established and specified by Microsoft to achieve the specified control objectives.

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft's controls were operating with sufficient effectiveness to achieve specified control objectives. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed.
- The results of Deloitte & Touche LLP's tests of controls.

The examination was conducted in accordance with the American Institute of Certified Public Accountants' (AICPA) Statement on Standards for Attestation Engagements No. 18 (SSAE 18). SSAE 18 is inclusive of the following: (1) AT-C 105, *Concepts Common to all Attestation Engagements*; (2) AT-C 205, *Examination Engagements*; and (3) AT-C 320, *Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control Over Financial Reporting*. It was also conducted in accordance with International Standard on Assurance Engagements 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Our testing of Microsoft's controls was restricted to the control objectives and related control activities listed in this **Section IV** and was not extended to controls described in **Section III** but not included in **Section IV**, or to controls that may be in effect at user organizations or subservice organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice organizations, and Microsoft's controls should be evaluated together. If effective user entity or subservice organizations controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

- Integrity and Ethical Values
- Microsoft SBC
- Training and Accountability
- Commitment to Competence
- OLC, IA Department, AC
- Risk assessment
- Information and communication
- Monitoring

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft's activities and operations, inspection of Microsoft's documents and records, and reperformance of the application of Microsoft's controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Tests of Operating Effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from October 1, 2020, through September 30, 2021. In determining the nature, timing and extent of tests we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the control objectives to be met, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Description of Testing Procedures Performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2020, through September 30, 2021. Our tests of controls were performed on controls as they existed during the period of October 1, 2020, through September 30, 2021, and were applied to those controls relating to control objectives specified by Microsoft.

In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period.

Tests performed are described below:

Test	Description
Corroborative Inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the reporting period to evidence application of the specific control activity.
Examination of documentation/Inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperfomed the procedures. Compared any exception items identified with those identified by the responsible control owner.

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information provided by the service organization to the service auditor in response to ad hoc requests from the service auditor (e.g., population lists); (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations); and (c) information prepared for user entities (e.g., user access lists), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard “out of the box” reports as configured within the system
- Parameter-driven reports generated by Microsoft’s systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Microsoft prepared analyses, schedules, or other evidence manually prepared and utilized by Microsoft

Our procedures to evaluate whether this information was sufficiently reliable included obtaining evidence regarding the accuracy and completeness included procedures to address (a) the accuracy and completeness of source data and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Microsoft.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Logical Access

Control Objective 1: Logical access controls exist to provide reasonable assurance that unauthorized access to key systems is restricted.

Control Activity	Tests Performed	Test Result
CA-33.a (1.01) - Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	<ul style="list-style-type: none">• Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted.• Identified population of users whose access had been modified or granted during the reporting period.• Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation.	No Exceptions Noted
CA-33.b (1.01) - Elevated access within the O365 production environment is approved by an authorized user.	<ul style="list-style-type: none">• Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted.• Observed and inspected the system configurations for elevated access within the O365 production environment to ascertain that elevated access is restricted to only approved individuals and is limited based on the established time constraints (for Just in Time Systems).• For Just in Time Systems - Observed for a sample of one user per just in time system that the individual was approved prior to access being elevated, and that the access duration was limited to the requested time.• For Standing Access Systems - Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-34 (1.02) - Identity of users is authenticated to Office 365 Services. The use of passwords incorporates policy on periodic change and password complexity.	<ul style="list-style-type: none"> Inquired of Logical Access control owners that authentication processes and password policies are enforced. Observed system configuration settings for a selected server for each service to ascertain that authentication policies regarding change intervals and complexity are being enforced. 	No Exceptions Noted
CA-35.a (1.03) - Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.	<ul style="list-style-type: none"> Inquired of the O365 team that processes have been established for identity access management system configuration to revoke access automatically based on account expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation. Obtained and inspected source code of the system configurations within the identity access management tools to corroborate that account expiration settings, including inactivity, Manager / Cost Center changes, and group settings are configured to remove access. Obtained and inspected system logs and tracking tickets for selected individuals that expiration settings were enforced, and access was removed based on the configurations within the identity access management system. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.b (1.03) - Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	<ul style="list-style-type: none"> Inquired of the O365 team that processes have been established for reviewing elevated access that is not automatically expired. Obtained and inspected user access review documentation for selected quarters to ascertain that access was reviewed, and any identified issues were addressed in a timely manner. With regards to the testing exceptions, obtained and inspected the alert logs for user access to the IC3 Azure environments supporting SfB and Microsoft Teams during the examination period to ascertain that no inappropriate access or changes were made during the period, and any alerts generated were tracked and resolved in a timely manner. 	<p><u>IDM</u> User access reviews were not properly documented from Quarter 1 through Quarter 3.</p> <p><u>WAC</u> For the selected Quarter 1 and Quarter 3 reviews, noted that two of 35 users marked for modification / removal were not removed in a timely manner during the Quarter 3 user access review.</p> <p><u>SfB / Microsoft Teams</u> The quarterly user access reviews supporting the Skype for Business and Microsoft Teams services did not include all relevant access groups related to its supporting services' Azure environments.</p> <p><u>All Other Services</u> No Exceptions Noted</p>

Control Activity	Tests Performed	Test Result
CA-36 (1.04) - Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	<ul style="list-style-type: none"> Inquired of Logical Access owners to gain an understanding of how authentication is enforced, and processes established with relation to encrypting communication with the production environment. Observed authentication to a selected production server to corroborate that two-factor authentication was required. Obtained and inspected source code configurations and system settings corroborating the encryption settings enforced for accessing the production environment. 	No Exceptions Noted
CA-43 (1.05) - When users no longer require access or upon termination the user access privileges are revoked in a timely manner.	<ul style="list-style-type: none"> Inquired of security management to gain an understanding of the process for disabling or removing access in a timely manner. Compared a listing of all terminated/ transferred users within the examination period with active user accounts in the O365 environments to ascertain if access for terminated/ transferred employees was revoked. Additionally, compared HR Termination reports to O365 security groups to ascertain that removals of terminated users were executed in a timely manner by comparing the users' termination dates against the date of access revocation. 	No Exceptions Noted
CA-37 (1.06) - Each Office 365 Service customer's content is segregated either logically or physically from other Online Services customers' content.	<ul style="list-style-type: none"> Inquired of security process owners to gain an understanding of the processes that enforce segregation, either physically or logically, of customer content. Obtained and inspected a sample of physical server configurations and tested user interfaces to ascertain that customer content is segregated. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-08 (1.07) - The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance (GRC) process owners that new and transferred Microsoft employees and contractors are required to undergo a background check prior to being granted access to the environment. Obtained and inspected background check data for a selection of Microsoft personnel to ascertain that a background check was performed prior to granting access to the production assets containing customer content. 	No Exceptions Noted

Complementary User Entity Control Considerations

- User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.
 - User entities establish proper controls over the use of system IDs and passwords.
 - User entities are responsible for managing their user's password authentication mechanism.
 - User entities enforce desired level of encryption for network sessions.
 - User entities manage anonymous access to SPO and SfB sessions.
 - User entities secure the software and hardware used to access O365.
-

Change Management

Control Objective 2: Changes to application programs and related data management systems are authorized, tested, documented, approved, and implemented consistent with management's intentions.

Control Activity	Tests Performed	Test Result
CA-03 (2.01) - Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.	<ul style="list-style-type: none">• Inquired of Governance, Risk & Compliance process owners to ascertain that Senior Management considers its commitments and requirements related to security, availability, confidentiality, and processing integrity as part of its major system release planning process.• Obtained and inspected evidence of the annual review including memorandums and planning meeting records, to ascertain that commitments and requirements for security, availability, confidentiality, and processing integrity were considered and approved by Senior Management, and these commitments and requirements were communicated to relevant personnel as part of the major system release planning process.	No Exceptions Noted
CA-18 (2.02) - Changes and software releases within the Office 365 environment are documented / tracked and are approved prior to implementation into production.	<ul style="list-style-type: none">• Inquired of Change Management control owners that procedures have been established and are followed prior to deploying changes to the production environment.• Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes are documented and tracked within a tracking tool.• Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes were approved by appropriate stakeholders prior to release	No Exceptions Noted
CA-20 (2.03) - Emergency changes to the production environment follow an emergency change approval process.	<ul style="list-style-type: none">• Inquired of Change Management control owners that deployed emergency changes are approved by identified key stakeholders prior to release into production.• Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that emergency changes were approved by identified key stakeholders.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-21 (2.04) - Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.	<ul style="list-style-type: none"> Inquired of Change Management control owners that testing of changes is documented and required for deployment into production. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that changes are tested prior to release according to established procedures. Obtained and inspected evidence for a selection of changes to ascertain that testing was reviewed and approved prior to release according to established procedures. 	<p>OSI Testing carried out for one out of twenty-five samples was not properly retained.</p> <p>All Other Services No Exceptions Noted</p>
CA-46 (2.05) - Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.	<ul style="list-style-type: none"> Inquired of SDL security process owners to ascertain that changes undergo a security review prior to release. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that a security review was performed prior to release for each build. 	No Exceptions Noted
CA-19 (2.06) - For teams utilizing the Developer / Operations model, monitoring processes or system configurations are in place to identify and remediate unapproved changes to production.	<ul style="list-style-type: none"> Inquired of Change Management and Logical Security control owners that for the teams using the Developer / Operations model, restrictions are in place to monitor or limit access to implement unapproved changes. Observed that monitoring is in place for developers with access to the environment. Obtain and inspected source code and change ticketing systems to ascertain that system configurations and procedures were in place to identify and remediate unapproved changes. 	No Exceptions Noted

Complementary User Entity Control Considerations

- None

Data Backup and Restoration

Control Objective 3: Data replication or backup controls exist to provide reasonable assurance that key information is replicated or backed up and can be restored in a timely manner.

Control Activity	Tests Performed	Test Result
CA-49 (3.01) - Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.	<ul style="list-style-type: none">Inquired of Data Backup and Restoration process owners that processes have been established for data backups and restorations.Obtained and inspected evidence for a selection of backups and replications to ascertain that data backups and replication were occurring according to defined procedures and alternative data instances were available for restoration or failover.	No Exceptions Noted
CA-50 (3.02) - Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines.	<ul style="list-style-type: none">Inquired of Business Continuity process owners to ascertain that failover tests occur on a regular basis.Obtained and inspected business continuity documentation and failover logs for a selection of failover tests to ascertain that the tests were completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution.	No Exceptions Noted
CA-51 (3.03) - Customer content and services are replicated to a geographically separate location.	<ul style="list-style-type: none">Inquired of Data Backup and Restoration process owners to gain an understanding of the process for locating customer content on replicated instances in geographically separate locations.Obtained and inspected system configurations and depending on the setup of the service, a selection of data sources, to ascertain that replicated instances reside in geographically separate locations.	No Exceptions Noted

Complementary User Entity Control Considerations

- User entities are responsible for enabling and maintaining email restoration for EXO.

Monitoring and Incident Management

Control Objective 4: The security of the environment is monitored to provide reasonable assurance that security vulnerabilities are detected and remediated.

Control Activity	Tests Performed	Test Result
CA-26 (4.01) - Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked in an incident tracking system.	<ul style="list-style-type: none">• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established.• Obtained and inspected evidence for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved.• Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review.• Obtained and inspected evidence for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted
CA-47 (4.02) - Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.	<ul style="list-style-type: none">• Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established.• Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved.• Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review.• Obtained and inspected incident documentation for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-27 (4.03) - There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.	<ul style="list-style-type: none"> • Inquired of Monitoring and Incident management process owners that processes for security vulnerability scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected security scanning reports for a selection of servers for evidence that vulnerability scans were being performed and completed successfully. • Obtained and inspected security scanning reports for a selection of servers to ascertain that scan results were being reviewed and issues noted were being tracked to resolution. 	No Exceptions Noted
CA-38 (4.04) - Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server's intended use.	<ul style="list-style-type: none"> • Inquired of Server Build-out management process owners that processes have been established to have baseline security and operational settings applied to all new servers deployed to the production environment. • Obtained and inspected system logs, source code configurations, and system change documentation for a selection of new servers to ascertain that baseline builds have been established, approved, and deployed prior to a new server being implemented in production. 	No Exceptions Noted

Complementary User Entity Control Considerations

- User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.

Network Services

Control Objective 5: Control policies and procedures provide reasonable assurance that network devices are maintained to address the latest security and operational risks.

Control Activity	Tests Performed	Test Result
CA-48 (5.01) – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards	<ul style="list-style-type: none">• Inquired of Microsoft Datacenters and Online Services Security & Compliance (OSSC) process owners that network devices are configured to log and collect security events and monitored for compliance with established security standards.• Observed that logging of security events is automated through a security log database. Additionally, observed security events from a sample server are logged as they occur in the security log database.• Obtained and inspected system configurations for a sample of servers and ascertained that the servers were configured to log and collect security events and those logs are monitored for compliance and any necessary items are resolved.	No Exceptions Noted
CA-39 (5.02) - User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.	<ul style="list-style-type: none">• Inquired of Global Networking Services (GNS) process owners to ascertain that procedures are in place for restricting access to Microsoft Datacenters managed network devices. Inquired that user groups have been created and enforced via the Active Directory.• Obtained and inspected a sample of network devices and inspected their configuration and tested that TACACS+/Radius are used for authentication, authorization of access and that ACLs have been applied.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-40 (5.03) - Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.	<ul style="list-style-type: none"> Inquired with the GNS process owners to ascertain that access to the network devices in the Microsoft Datacenters environment is restricted through a limited number of entry points which require authentication over an encrypted Remote Desktop connection. Inspected the GNS Account Management SOP and tested that procedures are established to restrict user access to Microsoft Datacenters - managed network devices in the scope boundary, through a limited number of entry points that require authentication over an encrypted connection. Selected a sample of Microsoft Datacenters - managed network devices and tested that remote access to network devices involves login to GNS RDG, using domain credentials and Smart card followed by login to internal-facing terminal server using domain credentials and Secure Shell (SSH) has been enforced to access the network device. Obtained the list of terminal servers and tested that access to network devices is restricted through a limited set of terminal servers. Selected a sample of network devices and inspected their configuration and tested that device access is restricted via above terminal servers. 	No Exceptions Noted
CA-41 (5.04) - Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms.	<ul style="list-style-type: none"> Inquired of GNS process owners to ascertain that two-factor authentication is enforced while connecting to a network device. Selected a sample of network devices and observed that login to these network devices required two-factor authentication. Inspected obtained supporting device configuration files for a selection of network devices to ascertain that they were configured to enforce two-factor authentication through TACACS+ or RADIUS servers. 	No Exceptions Noted
Complementary User Entity Control Considerations		
<ul style="list-style-type: none"> None 		

Customer Lockbox

Control Objective 6: Controls provide reasonable assurance that customer content is only accessed when authorized by a designated customer account administrator.

Control Activity	Tests Performed	Test Result
CA-56 (6.01) - Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.	<ul style="list-style-type: none">• Inquired of Operations and Security process owners to ascertain that Customer tenant administrators are notified when a Customer Lockbox elevation request is initiated to access their content.• Observed for a selected Customer Lockbox subscriber, that a Lockbox request was submitted and approved by tenant management.	No Exceptions Noted
CA-57 (6.02) - Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.	<ul style="list-style-type: none">• Inquired of Operations and Security process owners to ascertain that customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.• Obtained and inspected an access elevation log request and noted approvers were assigned to the request.• For a selected request, obtained and inspected access elevation logs to ascertain that an approval took place before access was granted.	No Exceptions Noted
CA-58 (6.03) - Customer Lockbox elevation requests to customer content require an associated service request.	<ul style="list-style-type: none">• Inquired of Operations and Security process owners to ascertain that Customer Lockbox elevation requests to customer content require an associated service request.• Observed that for an elevation request when a service request number was excluded, the elevation request failed to be processed.	No Exceptions Noted
CA-59 (6.04) - Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.	<ul style="list-style-type: none">• Inquired of Operations and Security process owners to ascertain Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.• Observed the population of Lockbox requests within the Office 365 Dashboard – Admin Center.	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-60 (6.05) - The workload where the content is accessed through Customer Lockbox logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that all servers that host customer content push audit logs to a repository on a real time basis. Observed for a sample elevation log that cmdlet activity was logged accordingly. Observed for a sample elevation that it can be identified through the Office 365 Dashboard search functionality. 	No Exceptions Noted
CA-61 (6.06) - Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that management reviews both Customer Lockbox and capacity server elevation. Obtained and inspected a sample of MSR monthly presentations which included elevation statistics and resolutions. Inspected that an approval was required in advance of an elevation request. 	No Exceptions Noted
Complementary User Entity Control Considerations		
<ul style="list-style-type: none"> When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner. 		

Section V:

Supplemental Information Provided by Microsoft

The information included in this section is presented by Microsoft Corporation (“Microsoft”) to provide additional information to user entities and is not part of Microsoft’s description of the system. The information included here in this section has not been subjected to the procedures applied in the examination of the description of the system, and accordingly, Deloitte & Touche LLP expresses no opinion on it.

Business Continuity Planning

The Microsoft Office 365 (“O365”) service incorporates resilient and redundant features in each service and utilizes Microsoft’s enterprise-level datacenters. These datacenters use the same world-class operational practices as Microsoft’s corporate line of business applications. The O365 team’s long experience in operating highly available services, combined with the company’s close ties to the product groups and support services, provides a comprehensive solution for the company’s online services with the ability to meet the high standards of its customers.

The company’s online services designs include provisions to quickly recover from unexpected events such as hardware or application failure, data corruption, or other incidents that may affect a subset of the user population. The company’s service continuity solutions and framework are based on industry best practice and are updated on a regular basis to support Microsoft’s ability to recover from a major outage in a timely manner.

Domain Name Services

O365 Domain Name Service (DNS) provides authoritative name resolution for a subset of public-facing domains associated with O365. These domains can be purchased by customers to rename their domain URLs.

Datacenter Services

The Microsoft Datacenters Management team has overall responsibility for the oversight of datacenter operations, including physical security, site services (server deployments and break/fix work), infrastructure build-out, critical environment operations and maintenance, and facilities management. Site Security Officers are responsible for monitoring the physical security of the facility 24x7.

The Microsoft Datacenter Management team conducts periodic operational reviews with the key third-party vendors that support the Microsoft Datacenters. The purpose of the operational reviews is to discuss the current state of agreed-upon deliverables. Third-party vendors have specific statements of work with service level agreements that are monitored for compliance and adherence. Statements of work are reviewed on a periodic basis and updates are made accordingly, as business needs require.

ISO/IEC Standards 27001:2013, 27017:2015, and 27018:2014

O365 is compliant with ISO standard 27001:2013 and meets the requirements of ISO 27017:2015 and 27018:2014, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO27000 series of standards were developed in the context of the following core principles:

“The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required).”

O365 has undergone the ISO 27001 certification process and has been certified by the British Standards Institute (BSI). To view the ISO/IEC 27001:2013 certificates, see the Certificate/Client Directory Search Results page located on the BSI Global website.

NIST 800-53 and FISMA

O365 implements security processes and technology that adhere to the NIST 800-53 standards required by US federal agencies and have acquired FedRAMP Authority to Operate (ATO) from multiple federal agencies.

Management's Response to Exceptions Identified

The table below contains Management's responses to the exceptions identified in **Section IV**.

Control Activity & Exception	Management's Response
CA-35.b (1.03) - Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	<u>IDM, WAC, SfB / Microsoft Teams</u> Logs of account usage have been reviewed. Confirmed that there has been no usage of the expired accounts since their last authorized usage date. Applicable teams have been reminded of this control requirement.
<u>IDM</u> User access reviews were not properly documented from Quarter 1 through Quarter 3.	
<u>WAC</u> For the selected Quarter 1 and Quarter 3 reviews, noted that two of 35 users marked for modification / removal were not removed in a timely manner during the Quarter 3 user access review.	
<u>SfB / Microsoft Teams</u> The quarterly user access reviews supporting the Skype for Business and Microsoft Teams services did not include all relevant access groups related to its supporting services' Azure environments.	
CA-21 (2.04) - Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.	Confirmed builds subsequent to the undocumented example followed required test procedures and found no residual faults. We have increased the retention time for this system.
<u>OSI</u> Testing carried out for one out of twenty-five samples was not properly retained.	



Microsoft Corporation—
Microsoft Office 365

System and Organization Controls (SOC) 2 Report

October 1, 2020, through September 30, 2021

Deloitte.

Table of Contents

Section I: Independent Service Auditor's Report	1
Section II: Management's Assertion	6
Section III: Description of the System	9
Section IV: Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities	36
Section V: Supplemental Information Provided by Microsoft	114

Executive Summary

Microsoft Corporation—Office 365

Scope	Microsoft Office 365 (O365) including Office 365 with International Traffic in Arms Regulations (ITAR) ¹ Support
Period of Examination	October 1, 2020, through September 30, 2021
Location(s)	Redmond, WA
Subservice Providers	Yes – <ul style="list-style-type: none">• Microsoft Azure (“Azure”) including Microsoft Datacenters
Opinion Result	Unqualified
Testing Exceptions	4
Complementary User Entity Controls	Yes – See Page 32
Complementary Subservice Organization Controls	Yes – See Page 34

¹ This report is a description of the “Microsoft Office 365 with ITAR Support system” (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

Section I:

Independent Service Auditor's Report

Microsoft Corporation
Redmond, Washington, 98052

Scope

We have examined the attached description of the system of Microsoft Corporation (the "Service Organization" or "Microsoft") related to its Microsoft Office 365, including International Traffic in Arms Regulations (ITAR)² Support, online services for processing user entities' transactions for the period October 1, 2020, to September 30, 2021 (the "Description") based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality ("applicable trust services criteria") set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The information in **Section V**, "Supplemental information provided by Microsoft," is presented by management of the Service Organization to provide additional information and is not a part of the Description. Information presented in **Section V** has not been subjected to the procedures applied in the examination of the Description and the suitability of the design and operating effectiveness of controls to achieve the Service Organization's service commitments and system requirements based on the applicable trust services criteria.

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage services. The Description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and system requirements based on the applicable trust services criteria. The Description presents the Service Organization's controls; the applicable trust services criteria; and the types of complementary subservice organization controls assumed in the design of the Service Organization's controls. The Description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated whether the controls management expects to be implemented at the subservice organization have been implemented or whether such controls were suitability designed and operating effectively throughout the period October 1, 2020, to September 30, 2021.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft, to achieve Microsoft's service commitments and

² This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

system requirements based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

The Service Organization is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion titled "Management's Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Service Organization is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design and operating effectiveness of the controls stated in the Description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other Than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the Description is presented in accordance with the description criteria, and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of those controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of those controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA, and accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The Description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of the controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are listed in **Section IV** of this report.

Opinion

In our opinion, in all material respects,

- a. The Description presents the O365 online services system of Microsoft that was designed and implemented throughout the period October 1, 2020, to September 30, 2021, in accordance with the description criteria.
- b. The controls stated in the Description were suitably designed throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively throughout that period and the subservice organization and user entities applied the complementary controls assumed in the design of the Microsoft's controls throughout that period.
- c. The controls stated in the Description operated effectively throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Microsoft's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in **Section IV**, is intended solely for the information and use of Microsoft, user entities of the in-scope services for Microsoft's O365 online services system during some or all of the period October 1, 2020, to September 30, 2021, business partners of Microsoft subject to risks arising from interactions with Microsoft's O365 system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.
- How the Service Organization's system interacts with user entities, business partners, subservice

organizations, and other parties.

- Internal control and its limitations.
- Complementary user entity controls and complementary subservice organization controls and how they interact with related controls at the Service Organization to achieve the Service Organization's commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the Service Organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Deloitte & Touche LLP

February 14, 2022

Section II: Management's Assertion

Microsoft Corporation's Assertion

We have prepared the description of the system in **Section III** of Microsoft Corporation ("Service Organization" or "Microsoft") throughout the period October 1, 2020, to September 30, 2021 (the "period"), related to its Microsoft Office 365, including Office 365 with International Traffic in Arms Regulations (ITAR)³ Support, online services ("O365"), based on criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* ("description criteria"). The description is intended to provide users with information about our system that may be useful when assessing the risks arising from interactions with Microsoft's system, particularly information about system controls that Microsoft has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("applicable trust services criteria").

The Service Organization uses Microsoft Azure including the Microsoft Datacenter service ("subservice organization") for its hosting of physical and virtual servers, network management, and data protection and storage services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls for O365, to achieve Microsoft's service commitments and system requirements related to O365 based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Microsoft's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Microsoft to achieve the service commitments and system requirements related to O365 based on the applicable trust services criteria. The description presents Microsoft's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Microsoft's controls.

We confirm, to the best of our knowledge and belief, that:

- a. The description presents Microsoft's system that was designed and implemented throughout the period October 1, 2020, to September 30, 2021, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft's service commitments and system requirements related to O365 would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Microsoft's controls throughout that period.

³ This report is a description of the "Microsoft Office 365 with ITAR Support system" (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

- c. The controls stated in the description operated effectively throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft's service commitments and system requirements would be achieved based on the applicable trust services criteria, if complementary subservice organization and user entity controls assumed in the design of Microsoft's controls operated effectively throughout that period.

Section III:

Description of the System

Overview of Operations

Business Description

Microsoft Corporation's ("Microsoft") Office 365 ("O365") service is a subscription-based business software service hosted by Microsoft and sold directly, or with partners, to various customers worldwide. O365 services are designed to provide performance, scalability, security, management capabilities, and service levels required for mission-critical applications and systems used by business organizations.

Customers subscribe to a standard set of features and services which are hosted in a shared, multi-tenant environment. This includes the Government Community Cloud, an Office 365 offering designed for US government customers. Also included is the Government Community Cloud High and Department of Defense offering, in which customers subscribe to a standard set of features hosted in a multi-tenant environment designed for the US Federal government, defense industry, aerospace industry, and government contractors to provide United States International Traffic in Arms Regulations (ITAR) support and meet Defense Information Systems Agency requirements.

O365 is physically hosted in Microsoft-managed datacenters. Microsoft Datacenters is an organization within Microsoft that provides hosting and network support solutions for the O365 environment. Microsoft Azure ("Azure") is an organization within Microsoft that provides supporting services for the O365 applications including authentication, virtual server hosting, and system data storage and protection. Microsoft Datacenters is managed and run by Azure and both services are treated as one subservice organization (Azure) but will be referred to separately in this report to clarify which part of the Azure organization is responsible for the different services. Both services are not within the scope of this report.

The following services are provided to all O365 customers:

- Email access and productivity tools
- Team communication and collaboration
- Document and other file storage
- Documents viewed and edited in a Web browser

O365 streamlines workflow for customers by providing them with added security, increased email accessibility, and easy team collaboration by providing hosted messaging and collaboration solutions.

Additionally, O365 is part of the Microsoft Cloud for Financial Services offering. Microsoft Cloud for Financial Services provides capabilities to manage data to deliver differentiated experiences, empower employees, and combat financial crime. It also facilitates security, compliance, and interoperability. This set of cloud-based solutions enhances collaboration, automation, and insights to streamline processes; personalizes every customer interaction; improves customer experience; and delivers rich data insights. The data model enables Microsoft's partners and customers to extend the value of the platform with additional solutions to address the financial industry's most urgent challenges. These capabilities will help organizations align to business and operational needs, and then deploy quickly to accelerate time to value. Microsoft Cloud for Financial Services and its capabilities (Unified Customer Profile, Customer Onboarding, and Collaboration Manager) are built atop Azure, Microsoft Dynamics 365, Microsoft Power Platform, and Microsoft 365 offerings. Azure, Microsoft Dynamics 365, Microsoft Power Platform are not part of the scope of this report.

Applicability of the Report

This report has been prepared to provide information on O365's internal controls that may be relevant to the requirements of its customers and affect the processing of user entities' transactions. The detail herein is intended to meet the common requirements of a broad range of users and may not, therefore, include every aspect of the system that each customer may consider important. Furthermore, detail is limited to the controls in operation over the system as defined in the O365 scope boundary described below. The authorized users of the system supporting the internal controls are limited to O365 personnel. This report covers the software offerings described in the sections below.

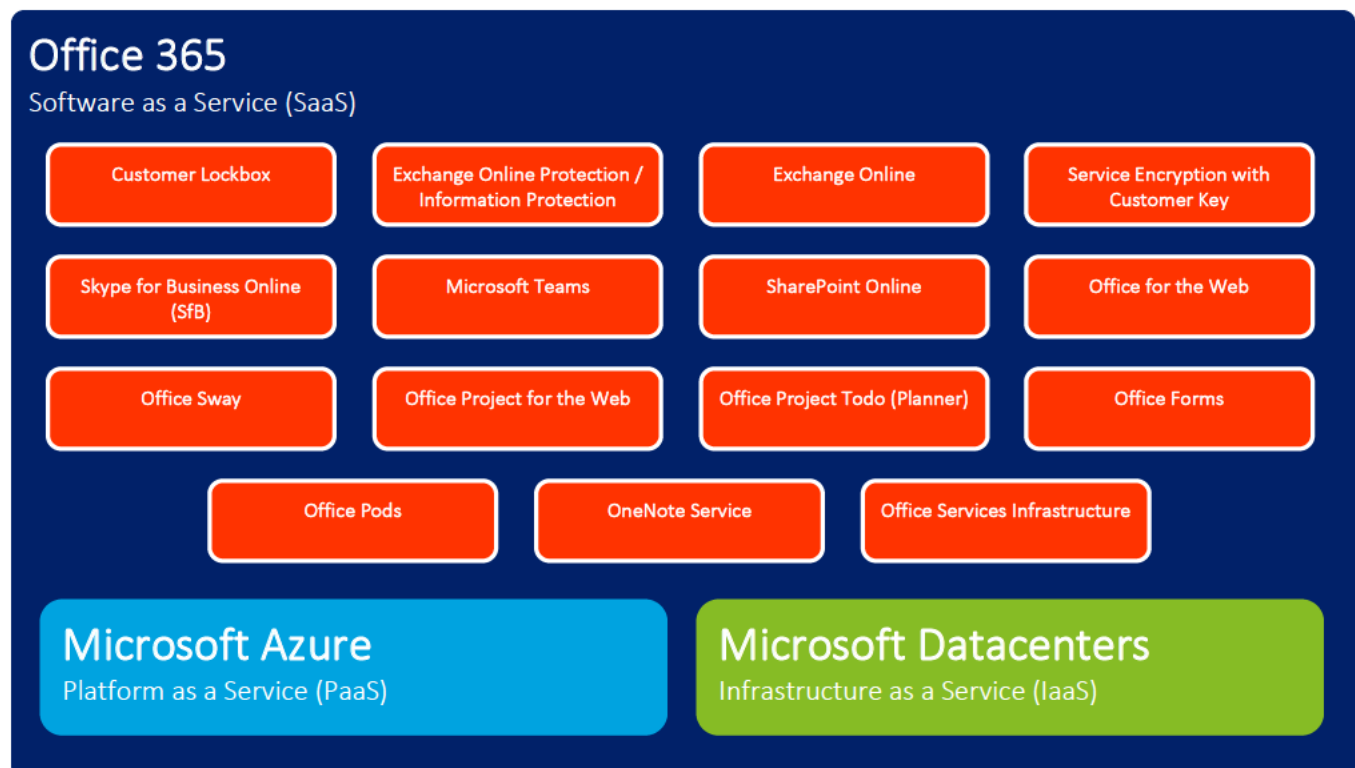
Infrastructure

All O365 services are hosted on a combination of the following subservice organizations within Microsoft: Microsoft Datacenters Infrastructure as a Service (IaaS) and Azure's IaaS and Platform as a Service (PaaS).

For Microsoft Datacenters hosting, the physical servers are owned by O365, the operating system (OS) and software are managed by O365, and network layer and network layer protections are implemented by Microsoft Datacenters. O365 manages the configuration of the network layer/protection in coordination with Microsoft Datacenters.

For Azure's IaaS hosting, O365 is responsible for the OS and database management. For Azure PaaS hosting, O365 is responsible for limited configuration of the OS while Azure is responsible for database and storage setup and maintenance, and overall OS setup and protections. Network layer protections are implemented by Azure for both IaaS and PaaS and are managed in coordination with Azure. Additionally, Azure manages the gateways for remote access into the O365 networks.

In both cases, Microsoft Datacenters is responsible for physical and environmental security. In addition, Azure PaaS provides customer authentication and rights management services through Azure Active Directory (AAD). The controls managed by Microsoft Datacenters and Azure are not in the scope of this report.



Software

O365 includes the following SaaS offerings:

- Customer Lockbox – An access control technology designed to provide customer control and transparency over access to customer content.
- Exchange Online Protection (EOP) – A service providing security features, such as antivirus, antimalware, and antispyware filtering for Exchange.
- Information Protection (IP) – A service providing security features, such as antivirus, antimalware, and antispyware filtering for Exchange. IP includes the following subservices: Adv eDiscovery, Compliance Manager and STP, Data Insights V2, Exact Data Match, Import service, Insider Risk Management, ML Inference, and O365 Auditing.
- Exchange Online (EXO) – An email service.
- Service Encryption with Customer Key – A service providing customers with two application-level encryption options for customer content at rest within the Exchange and SharePoint environments: Service Encryption with Microsoft-owned encryption keys and Service Encryption with customer-owned encryption keys (“Customer Keys”).
- Skype for Business Online (SfB) – A communication service that offers collaboration capabilities via instant messaging, audio and video calling, online meetings, and web conferencing.
- Microsoft Teams – A communication service that offers a threaded persistent chat experience that builds on O365’s group infrastructure, global scale, enterprise grade security, and graph driven intelligence. Microsoft Teams is also referred to as Azure Communication Service (ACS).
- SharePoint Online (SPO) – A solution for creating websites to share documents and information with colleagues and customers. This information and documentation repository includes OneDrive, Delve, Access Online, and Project Online.
- Office for the Web (WAC) (formally Office Online) – Enables users to access, view, and edit documents online via a web browser.
- Office Sway – Digital storytelling app for creating interactive reports, presentations, personal stories, and more.
- Office Project for the Web – Cloud-based work and project management.
- Office Project Todo (Planner) – Provides a visual way to organize teamwork and simplified task management.
- Office Forms – Create surveys, quizzes, and polls with real-time results, built-in response analytics, and export to Excel.
- Office PODS – PowerPoint Online Document Service (PODS) streams images representing slides or pages of an Office file to SharePoint on-demand.
- OneNote Service – Provides an Application Programming Interface to OneNote Notebooks on SharePoint.
- Office Services Infrastructure (OSI) – A platform for backend applications including deployment, hosting, and monitoring infrastructure applications.

O365 uses the following software to support the above offerings:

- Microsoft 365 (M365) Remote Access – A set of servers providing remote access to O365 service production environments via authorized two-factor authentication and encryption. This service was deprecated during the audit period and replaced with Azure Gateway, which is managed by the Azure subservice organization.
- Identity Manager (IDM) – An access management service providing an integrated and broad solution for managing O365 user identities and associated credentials for all O365 services (with the exception Microsoft Teams, which leverages MyAccess).
- Intelligent Conversation and Communications Cloud (IC3) – A supporting service for the SfB and Microsoft Teams services supporting first-party real-time conversation products including audio and video calling, meetings, and chat services.

O365 uses the following utilities to execute controls relevant to the O365 system:

- Employee Cloud Screening (ECS) – an SAP add-on used by Microsoft Human Resources that hosts employee background check information that synchronizes with IDM databases to limit user access to eligibilities based on background check status.
- Substrate, Office Substrate Pulse (OSP) – A platform and system tools for centrally managing and hosting applications and services that are used internally by O365 and by customers.
- Qualys – Scanning systems used to identify and resolve security vulnerabilities within the O365 environment.
- CorpFIM/IDWeb, MyAccess, and Torus – O365 user management tools used to grant temporary user access time-bound permissions and access to sensitive systems, including access to customer content.
- Remote Desktop Services – The accepted method for Microsoft personnel to gain logical access to the O365 environment remotely using Azure Gateway managed Remote Desktop Gateways (RDGs).
- Griffin/Office Supporting Infrastructure, O365SuiteUX Environments and Release Dashboard, PilotFish, and Azure DevOps – Change management tools used by service and support teams to track and deploy code changes to production environments.
- Aria, Avocado, Geneva, Incident Manager (IcM), Jarvis, and Heat Map – Dashboards and alerting systems that monitor the capacity and availability of the servers and services based on pre-determined capacity and availability thresholds. In the event of a breach of a capacity or availability threshold, automated alerts are generated and communicated to the service team's respective on-call engineer for tracking and remediation. Additionally, they provide a visual representation of major/minor system releases across various stages including preproduction, testing, and production.

People

O365 personnel are organized into service teams that develop and maintain the application and the support teams that provide supporting services for system operations.

Each service and support team for O365 has defined responsibilities and accountabilities to manage security, availability, processing integrity, and confidentiality of the applications. The teams include the following groups:

- Access Security – Personnel that maintain Active Directory (AD) services, authentication rules and user access.
- Change Management – Development, testing, and project management teams tasked with developing and maintaining the O365 applications and supporting services.

- Backups and Replication – Personnel for configuring and monitoring the replication and backup of specified internal and customer content.
- Security and Availability Monitoring – Personnel that monitor the incidents that affect the security and availability of O365 applications and supporting services.

In addition to service teams, centralized support teams provide specialized functions for the services, including the following:

- Enterprise Business Continuity Management (EBCM) – A single resource to assist O365 teams in analyzing continuity and disaster recovery requirements, documenting procedures, and conducting testing of established procedures.
- O365 Security – Manages cross-platform security functions, such as security incident response, security monitoring, and vulnerability scanning.
- Governance, Risk, and Compliance (GRC) – Identifies, documents, and advises teams in implementing controls to maintain O365's availability and security commitments to its customers.
- Office Trustworthy Computing (OTwC) – Develops and enforces the Secure Development Lifecycle process for O365 applications and support services.
- Identity Management (also known as Access Control team) – Operates the IDM tool to provide access control automation for all teams (excluding Microsoft Teams).
- Microsoft Information Technology (MSIT) – Provides the access control and authentication mechanism for Microsoft Teams via MyAccess.
- Azure – Provides customer authentication infrastructure including Microsoft Online Directory Services, Microsoft Organization ID, and AAD.
- Microsoft 365 Remote Access – Provides internal users remote access control and authentication to the O365 environment.
- Security Incident Response (SIR) – An internally focused resource that provides detection and analysis as well as containment, eradication and remediation for severe security incidents that may affect the O365 services.

Procedures

O365 adheres to Microsoft Corporation's Security Policy, which is owned by the Information Risk Management Council (IRMC), comprising business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) for Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses:

- | | |
|---------------------------------------|---|
| • Human resources security | • Systems acquisition, development, and maintenance |
| • Asset management | • Supplier relationships |
| • Access control | • Information security incident management |
| • Cryptography | • Business continuity management |
| • Physical and environmental security | • Compliance |
| • Operations security | |
| • Communications security | |

O365 uses National Institute of Standards and Technology (NIST) standard 800-53 for baseline control procedures, which are documented in the O365 control framework. Control measures above and beyond NIST 800-53 are included to address the full range of Microsoft contractual and regulatory commitments. The framework covers the following areas:

- Access Control
- Accountability, Audit, and Risk
- Authority and Purpose
- Awareness and Training
- Configuration Management
- Contingency Planning
- Data Minimization and Retention
- Data Portability
- Data Quality and Integrity
- Geographic Boundaries
- Identification and Authentication
- Incident Response
- Individual Participation and Redress
- Maintenance
- Media Protection
- Personnel Security
- Physical Access
- Program Management
- Risk Assessment
- Security
- Security Assessment
- Security Planning
- System Access
- System and Communication Security
- System and Information Integrity
- System and Services Acquisition
- Use Limitation

In addition to the above procedures, manual and automated control activities are described in the section “Description of Control Activities” below.

Data

O365 customer content is maintained in Azure and SQL server databases, which are hosted on a defined Windows AD domain. Each service and support team is responsible for managing the security, availability, processing integrity, and confidentiality of the data in Azure or on the database servers. The table below details the data classifications for this report and the O365 environment.

Data Classification	Definition
Access Control Data	Data used to manage access to administrative roles or sensitive functions.
Customer Content	Content directly created by users. Content is not viewed by Microsoft personnel unless required to resolve a ticketed service problem.
End User Identifiable Information (EUII)	Data unique to a user, or generated from a user’s use of the service: <ul style="list-style-type: none"> – Linkable to an individual user – Does not contain Customer Content
Organization Identifiable Information (OII)	Data that can be used to identify a tenant (generally configuration or usage data): <ul style="list-style-type: none"> – Not linkable to an individual user – Does not contain Customer Content
System Metadata	Data generated while running the service, which is not linkable to an individual user or tenant and does not contain Customer Content, EUII, OII, or Account Data.
Account Data	Administrator Data Payment Data Support Data

Control Environment

Integrity and Ethical Values

Corporate governance at Microsoft starts with a board of directors that establishes, maintains, and monitors standards and policies for ethics, business practices, and compliance that span the company. Corporate governance at Microsoft serves several purposes:

- To establish and preserve management accountability to Microsoft's owners by distributing rights and responsibilities among Microsoft Board members, managers, and shareholders.
- To provide a structure through which management and the board set and attain objectives and monitor performance.
- To strengthen and safeguard a culture of business integrity and responsible business practices.
- To encourage the efficient use of resources and to require accountability for the stewardship of these resources.

Further information about Microsoft's general corporate governance is available on the Microsoft website, www.microsoft.com.

Microsoft's Standards of Business Conduct

Microsoft's Standards of Business Conduct ("SBC") reflect a commitment to ethical business practices and regulatory compliance. They summarize the principles and policies that guide Microsoft's business activities and provide information about Microsoft's Business Conduct and Compliance Program. The SBC was developed in full consideration of the Sarbanes-Oxley Act of 2002 ("Sarbanes-Oxley") and NASDAQ listing requirements related to codes of conduct.

Further information about Microsoft's SBC is available on the Microsoft website, www.microsoft.com.

Training and Accountability

O365 leverages the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and to act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees (including O365), contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course upon being hired and again on an annual basis thereafter. In addition, employees are required to participate in mandatory security and compliance trainings periodically in order to design, build, and operate secure cloud services.

Microsoft O365 staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and applicable supporting standards. Individuals not employed by O365, but allowed to access, manage, or process information assets of O365 are also accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and associated standards.

Commitment to Competence

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and is used to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make appropriate hiring decisions.

Microsoft employees create individual accountabilities that align with those of their managers, organizations, and Microsoft, and are supported by customer-centric actions and measures so that everyone is working toward the same overarching vision. Accountabilities are established when an employee is hired and then updated throughout the year according to business circumstances.

Managers work with their employees to analyze progress against accountabilities and to adjust accountabilities, if needed, several times throughout the year. Managers evaluate individual contributions to teams, the business, or customer impact, taking into consideration contributions aimed at creating a high performing team and the demonstration of competencies relevant to the role.

Office of Legal Compliance — Board of Directors and Senior Leadership

The Office of Legal Compliance (OLC) designs and provides reports to the board of directors on compliance matters. The OLC also organizes annual meetings with the Senior Leadership team for its compliance review.

Internal Audit Department

Microsoft has an Internal Audit (IA) function that reports directly to the Audit Committee (AC) of the board of directors, which is constituted solely of independent directors. IA has a formal charter that is reviewed by the AC and management. The responsibilities of IA include performing audits and reporting issues and recommendations to management and the AC.

Audit Committee

The AC charter and responsibilities are on Microsoft's website, www.microsoft.com. The AC meets privately on a quarterly basis with Microsoft's external auditors and IA. The topics for the quarterly AC meetings are found in the AC Responsibilities Calendar set out in the charter. In addition, the AC influences the company through the IA function. The AC reviews the scope of IA and advises on the process of identifying and resolving issues. Lastly, the AC monitors itself by completing an annual self-evaluation.

Risk Assessment

Practices for Identification of Risk

IA, the Financial Compliance group, and the Finance Risk group perform formal risk identification processes each year. These assessments cover risks over financial reporting, fraud, and compliance with laws.

Internal audit — Fraud Risks

IA and the Financial Integrity Unit (FIU) look for fraud risk. The FIU performs procedures for the detection, investigation, and prevention of financial fraud affecting Microsoft worldwide. Fraud and abuse that is uncovered is reported to the Disclosure Committee. The FIU provides both a reactive and proactive response to allegations of fraud and abuse. The FIU uses a case management system that is also used by the Director of Compliance to track cases and related metrics. The FIU interacts with Microsoft management, Corporate, External, and Legal Affairs (CELA), HR, Finance, Procurement, and others to determine specific fraud risks and responses.

Periodic Risk Assessment

IA and other groups within the company perform periodic risk assessments. These assessments are reviewed by senior management.

IA specialization area leaders determine high-priority risks across the company, including risks related to financial reporting, operational business processes, and systems controls. Control failures are also analyzed to determine whether they give rise to additional risks.

Annual Risk Assessment

The annual risk assessment process is established to monitor, manage, and mitigate specific business risks related to security for customers and partners. Led by the Risk Management office, Microsoft follows an established approach to risk management and conducts an annual global risk assessment beginning in the first quarter of each fiscal year. The purpose of the annual risk assessment is to identify and prioritize each division's specific strategic and operational risks based on impact, likelihood, and management control. Additionally, accountability is established for each risk and mitigation decisions are made at the Corporate Vice President level with transparency across the leadership team.

OLC/IA/Risk Management — Risk Responsibility

The responsibility for risk is distributed throughout the organization based on each individual group's services. OLC, IA, and the Risk Management Group work together to represent enterprise risk management. Through quarterly and year-end reviews, the Chief Financial Officer (CFO) and Corporate Controller (and respective groups) review the disclosures and issues that may have arisen.

Information and Communication

Internal Communication

Responsibilities concerning internal control are communicated broadly, which includes Monthly Controller calls, All Hands Meetings run by the CFO, and update conference calls held by the Financial Compliance Group with the Sarbanes-Oxley extended project team. Responsibilities for compliance with policies are set out in the SBC for which a mandatory training has been established for all employees. Additionally, compliance managers meet with control owners to make sure they understand the controls for which they are accountable and update the controls based on changes in the business environment.

Office of the CFO — Communications External to the Company

CFO communications outside the company occur throughout the year and, where applicable, these external communications include discussions of the company's attitude toward sound internal controls. The Office of the CFO is responsible for several communications outside of Microsoft including quarterly earnings releases, financial analyst meetings, customer visits, outside conferences, and external publications.

Monitoring

OLC — Business Conduct Hotline

There is a confidential and anonymous Business Conduct Hotline available for employees to report issues. The hotline is accessible 24 hours per day and 7 days per week through email, phone, fax, and mail. The individual may also send a letter or fax reporting the concern to Microsoft's Director of Compliance. Employees are instructed that it is their duty to promptly report concerns of suspected or known violations of the Code of Professional Conduct, the SBC, or other Microsoft policies or guidelines. The procedures to be followed for such a report are outlined in the SBC and the Whistle Blowing Reporting Procedure and Guidelines in the Employee Handbook. Employees are also encouraged to communicate the issue to their manager, senior leadership, CELA contact, HR contact, or the Compliance Office.

Internal Audit

Microsoft's IA department provides support to management across the company by independently and objectively analyzing whether the objectives of management are adequately performed, as well as facilitating process improvements and the adoption of business practices, policies, and controls governing worldwide operations.

Monitoring of Subservice Organizations

O365 uses Microsoft Azure including the Microsoft Datacenter service, which manages datacenters, IaaS, and PaaS supporting services for the O365 applications including hosting of servers, network support, authentication, virtual server hosting and system data storage. Note that O365 considers Azure and Microsoft Datacenters as two separate organizations within this report and are defined as such.

The O365 GRC team is responsible for identifying dependencies of each service and monitoring the subservices implementation of agreed-upon security, availability, processing integrity, and confidentiality controls. Dependencies are documented in Inter-Service Agreements. Monitoring includes, but is not limited to, the review of third-party service auditor reports and discussions with subservice organization management.

A brief overview of the subservice organizations used by Microsoft O365 is below.

Organization	Brief Description
Microsoft Azure	Microsoft Azure's cloud PaaS offerings are used by O365 to host production data and handle logical access and change management controls for O365.
Microsoft Datacenters	Microsoft Datacenter's IaaS offerings are used by O365 to host physical and virtual servers and system data storage. Microsoft Datacenters also handles physical and environmental security controls for O365.

Description of Control Activities

This report leverages the TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, Trust Services Criteria). The description of control activities relevant to the trust criteria are included below. Additionally, the criteria for each principle and the relevant O365 controls in place to satisfy the criteria are included as part of "Part A" in **Section IV** of this report and are an integral part of the description of the system.

Business Planning

The O365 planning process is driven by product updates and releases. Senior management defines the vision and strategy for the overall O365 product on an annual basis. During this process, senior management considers its high-level commitments and requirements to security, availability, processing integrity, and confidentiality in a series of planning meetings and communicates the output to O365 personnel through a strategy memo. The O365 Development and Project Management team leads also consider their teams' commitments to security, availability, processing integrity, and confidentiality on a more specific level and communicate the outcome in component planning meetings. These commitments are then converted into design considerations for implementation during the product releases. Implementation of these requirements is advised by the O365 Security team, which is responsible for overseeing security issues, system operation, and service availability within the O365 environment. In addition, an O365 GRC risk team has been defined and is responsible for management of security, availability, processing integrity, and confidentiality controls within the O365 environment. Finally, service teams have personnel who are responsible for system operation, service availability, and control implementation. Each team works to implement and maintain the commitments for security, availability, processing integrity, and confidentiality.

Hiring Process

Microsoft hiring managers define job requirements prior to recruiting, interviewing, and hiring. Job requirements include the primary responsibilities and tasks involved in the job, background characteristics needed to perform the job, and personal characteristics required. Once the requirements are determined, managers create a job description, which is a profile of the job, and use it to identify potential candidates. When viable candidates are identified, the interview process begins to evaluate candidates and to make an appropriate hiring decision.

Performance Review

Microsoft employees create individual accountabilities that align with those established for their manager, organization, and Microsoft. Each accountability is supported with customer-centric actions and measures so that

O365 personnel are working toward the same overarching vision. Accountabilities are established when an employee is hired and then updated throughout the year according to business needs.

Periodically, performance reviews, called "Connects", are held between employees and their managers, during which progress is analyzed against accountabilities and accountabilities are adjusted, if needed. The manager evaluates the individual's contributions to the team and business or customer impact, taking into consideration contributions towards creating a high performing team and the demonstration of competencies relevant to their role.

Standards of Business Conduct

O365 leverages the Microsoft Corporate SBC to provide employees with education and resources to make informed business decisions and act on their decisions with integrity. SBC training and awareness is provided to Microsoft employees (including O365), contractors, and third parties on an ongoing basis to educate them on applicable policies, standards, and information security practices. Full-time employees must also take a mandatory SBC training course upon being hired and again on an annual basis thereafter. In addition, employees are required to participate in mandatory security and compliance training periodically in order to design, build and operate secure cloud services.

Background Checks

Backgrounds checks are required for all US based full-time employees and vendors before access is granted to certain eligibilities within each workstream. US Background checks are renewed every two years. Microsoft has rolled out an international screening program, which requires background screening and renewals for all new FTE and vendor personnel in forty-four countries, as permitted by the laws of each country.

Microsoft full-time employees request background checks, when necessary, through the OSP employee portal. A notification is sent to the requesting employee's manager for approval. If approved, a notification email is sent to Microsoft HR to process a background check for the requesting employee. When the background check is complete, HR enters the results into ECS.

For vendors and contractors, vendor companies are responsible for completing a valid background check for each contracted vendor. Once completed, Microsoft receives an attestation letter from the vendor company confirming the completion and pass status of the vendor's background check. Once the background check validation is received, Microsoft enters relevant information into ECS. Background check information for FTEs and vendors is pushed from ECS to an IDM database, after which the IDM tool checks for employee background check information before access to O365 cloud environments can be requested by the employee. Full and incremental sync jobs run to keep the data used by the IDM tool current.

Workload administrators configure requirements, including background check, for eligibilities within each workstream. If no background check is on file, or if a background check has expired, the user receives an error indicating that the employee does not have required background check, thus preventing the employee or vendor from obtaining those eligibilities.

System Description

Information regarding the design and operation of O365, including Service Level Agreements (SLAs), is available to customers on the Internet in many locations, including www.microsoft.com. Additional system description details are available for customers and potential customers through third-party audit and attestation reports as well as control documentation through the Service Trust Portal in the Admin Portal. A specific view of the O365 environment is used internally to analyze key processes for system operation.

Customer Commitments and Responsibilities

Externally, O365 communicates its commitments, including those related to regulations, security, availability, processing integrity, and confidentiality to customers through contracts and SLAs. Internally, these commitments are reflected in a control framework, which is refreshed on an annual basis with control owners. These commitments and the associated control framework are distributed to O365 employees through policies, training, and Office Hours. Office Hours are twice-weekly time slots set aside during which O365 teams may speak with the GRC team to discuss topics including security, availability, and regulatory information, and how that information could impact their relevant areas of the control framework.

In addition to communicating commitments to its customers, O365 communicates the responsibilities of the customer to use the services. These responsibilities are described in SLAs, contracts, audit and attestation reports issued by independent auditors, and through descriptions available on Microsoft websites.

Policies

All Microsoft O365 staff and contingent staff are accountable for understanding and adhering to the guidance contained in the Microsoft Security Policy and applicable supporting standards. Individuals not employed by Microsoft but allowed to access, manage, or process information assets of Microsoft are also accountable for understanding and adhering to the guidance contained in the Security Policy and Standards. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification, risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the Microsoft intranet.

Security and Availability Incident Communication

O365 has established incident response procedures and centralized tracking tools, which consist of different channels for reporting production system incidents and weaknesses. Security and availability monitoring tools include Qualys, and Office Substrate Pulse. Incidents may also be reported via email by different O365 teams or Microsoft groups, such as the specific application and supporting services teams, Azure teams, or Microsoft Datacenters teams. The security teams operate 24x7x365 event/incident monitoring and response services.

External users may communicate security and availability incidents to Microsoft and receive updates through Customer Support, the online customer portal, or the customer service number.

Service Infrastructure and Support Systems Change Management Communication

Customers may view prior or upcoming upgrades and changes to the O365 service infrastructure in the Microsoft O365 blog. In addition, O365 customers receive notifications of major changes prior to change implementation through the customer portal. See the section “Service infrastructure and support systems change management” below for a description of the overall infrastructure and application change management process.

Risk Assessment – O365

O365 performs an annual risk assessment that covers security, continuity, and operational risks. As part of this process, threats to security are identified and the risk from these threats is formally assessed. The information gained from the assessment is used to create and prioritize work items.

O365 is represented on the Operational Enterprise Risk Management (OERM) Governance Committee by the O365 Risk Management Office. For O365 the risk review is done annually, beginning in August. O365 risk management contacts the O365 GRC working group directly for updates to the overall environment and discussion of risk issues identified during the assessment process. The result of these procedures is a report sent

to the corporate Vice President of the Office Product Group for review and approval. O365 risk management also sends information to the OERM for inclusion in the annual report that is sent to the Microsoft Board of Directors in December.

Control Design and Implementation

Based on the risk assessment performed, control activities are put in place within the O365 control framework. This framework is managed by the O365 GRC group and is evaluated and updated on an ongoing basis. This evaluation includes input from changes to the overall O365 environment, the regulatory landscape, and results of control assessments.

Implementation of the control activities is the responsibility of each of the O365 application and supporting service teams.

Data Flow Diagrams

Data flow diagrams showing O365 system interactions and dependencies are maintained for each service. On a semi-annual basis, these diagrams are updated by GRC personnel with the input of relevant service teams. This is done to provide up to date O365 system design information to O365 personnel to provide them with an understanding of their role in the system and additional background for addressing system security, availability, processing integrity, and confidentiality-related issues.

Control Monitoring

The design and operating effectiveness of security, availability, processing integrity, and confidentiality controls are analyzed by a third party at least once per year. These assessments include external (e.g., ISO and FedRAMP audits) and internal evaluations (e.g., risk assessments and vulnerability scans). The results and findings from these assessments are addressed with corrective actions, which are tracked by the O365 GRC team to substantiate that they are addressed in a timely manner.

Access Management

Microsoft O365 environments use an AD infrastructure for centralized authentication and authorization to their systems and services. There are multiple identity access management tools used by the service teams to manage their respective AD domains.

Identity Access Management

Microsoft O365 owns and manages tools that regulate access to O365 production environments. Most service teams use the IDM access management service to limit access to authorized users. The service, managed by the Access Control team, allows each of the other service teams to manage their respective AD clusters for their respective environment. Several backend processes synchronize with other internal Microsoft tools, such as Microsoft HR department systems, to check that user information (e.g., employment status, manager, cost center, background check information) meets predefined requirements. Users who meet predefined criteria can request access to certain eligibilities, and access is only granted after approval.

Some access is regulated outside the IDM service via other tools and processes; however, the functionality and processes are the same. These tools include IDWeb and MyAccess.

New User or Modification of User access

The process to request and approve new access via access management tools is managed through automated workflows configured within the tools. The systems automatically route access requests to the requestor's manager for approval. Users who meet specified requirements (e.g. active user, active manager, applicable cost

center, or background check) can request specific access to rights within each environment. User requests trigger notifications to the user's manager via email of a pending access request requiring manager approval. No access is provisioned within production environments until manager approval is obtained.

There are certain groups, roles, or entitlements that fall outside the automated provisioning processes described above. In each case users must still submit access requests, and each request must be approved before the access is manually provisioned.

External Users (Customer Entities) – When a new customer is added to the O365 service, they are provided with an initial account for system setup. The provisioning of users and deactivation of users is the responsibility of the customer entity.

Termination Access Removal

When individuals leave the company, Microsoft HR updates the terminated employee's details in the HR system, which syncs to access management tools via backend tasks. Access for terminated employees is then removed from respective service production environments. Without the appropriate entitlements, the user cannot access services within the O365 environment.

Periodic User Access Review

Services using the automated access provisioning processes above rely on workflows within the systems to automatically revoke user access based on the following criteria:

- Inactivity - after 56 days of inactivity, the user's account is disabled.
- Manager Change - when a user's manager and/or cost center has changed, users must re-request access using the same process described above, and the new manager must approve the user's requested access.
- Group Pre-defined Expiration - Where applicable, workloads have security groups that have a set expiration period from when an account was granted access to the group.

For manually maintained user access, a manual user access review is performed on a periodic basis to substantiate that access for each user is relevant and in line with job responsibilities. Any needed access alterations identified during the review are addressed in a timely manner.

Just-in-Time Access

Just-in-time (JIT) tools allow individuals to request temporary elevated access privileges on an as-needed basis to limited areas within the respective service team's associated Windows AD environments.

Each tool follows a similar process before granting temporary elevated access to requesting engineers. Automated configurations within each tool notify the submitting user's manager with details of the access requested. If approved, the requesting user is granted access on a temporary basis, and the tool automatically removes the requested access based on built-in functionality within the tool. In certain cases, an engineer may receive a one-time preapproval for access elevations to specific areas within an environment; however, the access is still temporary in duration. Additionally, each elevation is logged and retained by the service team for incident evaluations.

Developer/Operations Model - Developer Access to Production

Using the Access tools described above the service teams have restricted access to appropriate personnel, including the enforcement of segregation between developers and operations personnel.

Select service teams allow developers temporary access to production using the JIT tools and approval processes described above. Developer access is limited to specific areas of the environment for deployment or operations purposes. These limitations are enforced using Torus, a Remote PowerShell tool. Torus allows for the restriction of access to specific commands that can be run in the service team's environment and requires approvals for each command being requested. The Torus request and approval process is managed by the JIT tools described above. For requests to make changes to production code or data by a developer or operator, an associated service request ticket must be provided and approved by a separate individual.

Authentication

Internal users are authenticated using Remote Desktop Services and must be authenticated using a two-factor authentication mechanism that includes a smartcard with PIN to log into the RDG. After logging in to the RDG, the user must enter his/her production account user ID and password to access production servers. The corporate password requirements are defined and configured in each service teams' and support teams' Windows AD domain. These requirements include password complexity, length, history, and duration. Additionally, internal users can gain temporary access to elevated roles allowing access to customer content via the JIT methods described above. For those services that only use JIT elevations to access the environment with no standing access, there are requirements built into the JIT tools for generating onetime complex passwords for authenticating into these environments.

External Users – Microsoft provides various options to enable the authentication mechanism for end users and O365 customers. Each external entity is responsible for substantiating that the mechanism is configured and operating, as well as enforcing the use of strong passwords.

Mobile Devices

For Microsoft employees and other internal users, access to O365 applications and supporting services infrastructure through mobile devices is restricted and managed by the Microsoft Datacenters group.

External users – External users will go through the same authentication process to access O365 applications regardless of device. The external users' access is managed and configured by the customer.

Customer Lockbox

Customer Lockbox is an access control technology included in O365, designed to provide customer control and transparency over access to customer content hosted in Microsoft datacenters. The service grants Microsoft engineers temporary access to customer content on as-needed basis only as approved by an appropriate tenant authority. The following sections, prefixed with "Customer Lockbox," detail the procedures in place to limit Microsoft access to customer generated content.

Customer Lockbox - Authorization and Notification

Access to customer content for customers utilizing the Customer Lockbox feature, is initiated through a Service Request made via Microsoft's customer support. If the Service Request requires access to customer content, the access is requested through the Customer Lockbox tool. Individuals who are approved to access the customer content do so using the Remote PowerShell (RPS) tool.

Only Microsoft engineers with appropriate access entitlements within the Exchange environment, can request temporary elevation to the 'AccessToCustomerData' role, which allows access to customer content. The request process is built into Customer Lockbox. If approved by the role owners, Microsoft managers, the request is then routed to a customer contact for additional approval.

Customer Lockbox - Customer Approval

The automated workflows supporting the Customer Lockbox elevation process require that elevation requests are first approved by Microsoft management before being submitted to a tenant administrator. Tenant administrators are assigned and are the responsibility of each customer. If the request is not approved within a specified period of time by both the Microsoft management and the tenant administrator, then the elevation request times out and becomes invalid.

Customer Lockbox - Associated Service Request

Each elevation request made using Customer Lockbox must reference an associated service request number before submission to Microsoft management for approval. Attempts to submit an elevation request without an associated service request number will fail, and the RPS tool will return an error. Service requests are either submitted by the effected customer or created and communicated to the customer prior to the elevation request.

Customer Lockbox - Office 365 Admin Center

O365 customers can review a history of Customer Lockbox elevation requests within the customer's O365 Admin center. The history includes relevant information for current and past elevation requests, including the date, service request number, duration of elevation, reason for elevation, and requestor. The logs are kept for a reasonable period of time.

Customer Lockbox - Searchable Audit Logs

Server activity is logged for each Customer Lockbox elevation, and the activity log repository is available to each Customer Lockbox customer. Activity logs show what actions and commands were executed on a server containing customer content by a Microsoft engineer for the time allowed during an elevation requested through Customer Lockbox.

Customer Lockbox - Management Review of Elevations

Microsoft management pulls logs of Customer Lockbox elevations, as well as capacity server administrator elevations, from a data repository and investigates any anomalies. The statistics are reviewed as part of a Monthly Service Review with Microsoft management. For customers who have chosen to use Customer Lockbox, it is the only way to access customer content. Any other access paths are considered malicious access and are not covered by this attestation.

Data Management

Data Transmission (Encryption)

Encryption between Microsoft employee and datacenter connection

RDG connections are configured to establish Secure Socket Layer (SSL) connections between the internal users and the server hosted within the associated AD domain. The SSL encryption algorithm is Federal Information Processing Standard (FIPS) 140 compliant.

Additionally, access to the O365 applications and support services environments by Microsoft employees to both the RDG and the workload servers is encrypted using the defined encryption settings and protocols described above. This encryption is managed by the M365 Remote Access team.

Encryption between client and Microsoft datacenter connection

Based on the customer's data connection request, the encrypted connection is configured through the Microsoft network between the client and the desired O365 application and support services. The encryption levels are set by the customer, but each O365 service team has a specified and maintained listing of allowable encryption protocols that the customer may use.

Encryption between Microsoft datacenters

Each service team is responsible for establishing secured and encrypted connections across datacenters. Teams that use an Azure PaaS subscription rely on Azure to configure and manage encryption settings.

Data at Rest (Encryption)

Customer content at rest in the O365 environment is encrypted at rest utilizing full disk encryption or file level encryption. The data is encrypted using BitLocker for disk level encryption and custom code built into the applications and supporting services for file level encryption. For example, SPO encrypts at the per-document level, and EXO has begun rolling out mailbox level encryption. Additionally, teams that store data on Azure Blob storage utilize Azure's built-in encryption at rest.

Data Segregation

Customer content is stored and processed on a shared database which is logically segregated using program logic and a different customer identifier.

Service Encryption with Customer Key in Office 365

Microsoft O365 provides customers with two application level encryption options for their data within Exchange and SharePoint service: 1) Service Encryption with Microsoft owned encryption keys, and 2) Service Encryption with customer-owned keys ("Customer Keys").

In the standard Microsoft Service Encryption described above, O365 owns the encryption keys for the customer's Exchange mailboxes and SharePoint sites. Service Encryption with Customer Key ("Customer Key") is an opt-in encryption offering that allows O365 customers to supply and manage their own encryption keys for advanced, self-managed protection. The Customer Key offering is available in both the Exchange Online Worldwide, GCC-M, GCC-H, Department of Defense environment, as well as the SharePoint Online Worldwide environment.

Each "Customer Key" subscription a customer maintains has its own service tenant encryption identifier, and two corresponding Azure-hosted customer key vaults. The customer keys are housed in Azure Key Vault; the onboarding process is inclusive of an Azure subscription creation, which customers will then use to house their keys which correspond with their "Customer Key" service. The two respective Azure Key Vaults each maintain a unique encryption key provided by the customer during the "Customer Key" onboarding process.

For EXO: The "Customer Key" model can be applied to all users within a customer's AD environment or can be segregated based on customer preferred user groupings or business unit differentiations. Each respective Exchange "Customer Key" subscription instance maintains its own Data Encryption Policy ("DEP") that must be configured by the customer admin during the onboarding process as well. Once a DEP has been created, the customer can provision AD user mailboxes to that DEP, applying that encryption policy to the user mailboxes provisioned to that Customer Key DEP.

For SPO: The Customer Key model is applied at the tenant level via Tenant Intermediate Keys "TIKs"; if a customer opts-in to Customer Key, all SharePoint site instances are encrypted at the application layer.

Customer mailboxes or SharePoint sites associated with a Customer Key DEP or TIK are only accessible through utilizing the customer root keys relevant to each encryption policy type, which are stored in Azure Key Vault. Through Azure, Microsoft maintains its own interim keys, but an interim key does not have the ability to decrypt customer data. Under rare circumstances, Microsoft may need to access resources with customer content to perform specific service oriented and maintenance tasks.

Do to this the service performs a customer key wrap operation, in which Microsoft's interim key is sent to Azure blob storage to be wrapped with a data blob of the customer key. The Azure key wrap function does not allow Microsoft access the unique customer root keys themselves; the interim keys are instead wrapped with the root key data for access purposes. Once retrieved, the Microsoft engineer can access resources with customer data to

perform the relevant service tasks. Once the tasks are complete, an unwrap operation is performed, in which the wrapped interim key is sent to Azure blob storage to be unwrapped and consequently disassociated from the customer root key housed in Azure Key Vault. Unwrapped interim keys cannot access Customer Key encrypted data.

Microsoft provides additional protections if the customer owned root keys are lost or stolen with an “Availability Key”, which provides O365 customers with the capability to recover from the unanticipated loss of root keys. Microsoft will either assist customers through this process or provide customers with instructions on how to recover without assistance from Microsoft.

The Availability Key is a root key that is provisioned and protected by Microsoft and is functionally equivalent to the root keys that are supplied by the customer for use with service encryption with “Customer Key.” Because the Availability Key is protected by Microsoft, it uses a different security design and controls from keys that the customer manages. This provides defense-in-depth and protects against the loss of all keys from a single attack or point of failure. Sharing the responsibility to protect the keys, while using a variety of protections and processes for key management, ultimately reduces the risk that all keys will be lost or destroyed.

Service Encryption with Customer Key in Office 365 – Termination

Customers can opt out of the Service Encryption with Customer Key service. For EXO, customers can revoke root key access, either through group divestiture at a DEP level or through full-service exit. Since the TIK applies to all SharePoint instances, opting out of the Customer Key service consequently applies to all of the tenant’s SharePoint instances.

When a tenant wishes to opt-out of the Service Encryption with Customer Key service, the Exchange and SharePoint tenant administrators must confirm that the customer is truly opting out of the service and wants the data to be deleted. Once a customer opts-out of the service, deletes their own root keys, and signs the eDocument stating their service termination, Microsoft locks the customer out of their data as a confirmation step that the tenant would truly like that data to be deleted. Once this step has been taken, the customer’s executive team must formally communicate the opt-out decision on behalf of the customer via signed and notarized documentation. Microsoft will maintain their root key to the customer’s data until the executive confirmation of service termination has been received, or the 90- to 180-day deletion period threshold has been reached. Once the customer service termination confirmation has been communicated, the customer can request that Microsoft delete its root key access to the data in question.

Network Management

Network Problem Management

Microsoft Datacenters’ Global Networking Services (GNS) has designated teams (i.e., Problem Management, Network Escalations, and Network Security) to identify and address security alerts and incidents. GNS is responsible for identifying and analyzing potential problems and issues in the Microsoft Office 365 Services networking environment.

Network Configuration Monitoring

Microsoft Datacenters’ GNS team has implemented procedural and technical standards for the deployment of network devices. These standards include baseline configurations for network devices, network architecture, and approved protocols and ports. GNS regularly monitors network devices for compliance with technical standards and potentially malicious activity.

Network Change Management

GNS has implemented a formal change management process that requires network changes, including configuration changes, emergency changes, Access Control Lists changes, and new deployments to be

documented and authorized prior to implementation. Changes and change approvals are tracked in a ticketing system.

Server/Network Device Remote Access

Microsoft Datacenters provides remote server and network device access to Microsoft Datacenters-managed environments. Access is provided through Microsoft Datacenters-managed Active Directory security groups and follows standard logical access procedures as established by Microsoft Datacenters and GNS.

Server Build-out Process

O365 has a defined server build-out process to deploy and configure new servers and rebuild existing servers. As part of the server build-out process, each service team performs the following:

- Connect the server to the specified AD domain.
- Install antimalware agents to get up to date antimalware signature files and definitions.
- Install a server agent to collect server activities and upload the logs to the Security Incident Response (SIR) team databases for security assessment activities.

After the base server image is applied and the related build-out process is finished, quality assurance reviews are conducted to validate that the server build-out process completed as expected. The quality assurance review follows one of two processes for server build-out compliance:

- Quality assurance checklist/Automated scan:

As part of the build-out process, each server is scanned using an automated tool. This scan produces a log file that details if the applicable build-out steps were followed and completed successfully. In addition to this scan, teams follow a manual checklist to ascertain that some steps have been completed in the build-out process, which includes evaluating the automated scan log file.

- Automated build-out tool:

Application and supporting service teams that leverage an automated build-out and deployment process utilize a scan performed by the deployment tool to substantiate the build had completed successfully. If there is a failure, the tool attempts to redeploy the build until successful.

Certain services leverage Microsoft's Azure PaaS offerings for server build-out and management. Teams who use Azure IaaS with customized server images maintain, update, and test server images as part of the deployment process. Once the server image has been tested, it is provided to Azure for actual deployment.

Antimalware

Through the server build-out process, each application and supporting service has an antimalware agent installed. The antimalware agent is configured to obtain the latest available definition files on the master antimalware server hosted within the service team's AD domain. If there are issues related to the agent synchronization process with the master server, the individual server's antimalware agent automatically notifies the SIR team, and the reported issue is analyzed and resolved.

Vulnerability and Patch Management

The O365 Security team monitors for known configuration and patching vulnerabilities through automated scans based on Qualys technology. A master server is configured to scan each server within O365 applications and supporting services AD domains to analyze and report known vulnerabilities and patch non-compliance. Each service team reviews the vulnerability scan report from the master server and assesses the criticality of the vulnerabilities and applies patches as applicable.

New vulnerabilities (e.g., those from responsible disclosure programs) are communicated to O365 through the Microsoft Security Response Center. If a patch is developed for the vulnerability, each service team evaluates the relevance of the patch to its environment and applies the patch as applicable.

Security Incident Monitoring

O365 has implemented incident response procedures, which consist of technical mechanisms, organizational infrastructure, and other procedures to detect, respond, and deter security incidents. The O365 incident management technical infrastructure includes monitoring systems for detecting and alerting O365 personnel of security events and incidents. A monitoring agent is installed on each server at the time of server build-out to transfer the security logs to the Security Incident Response (SIR) team, which identifies potential incidents and serves as a central repository for investigations. Incidents posing significant risk to the environment are prioritized for response and mitigation.

Additionally, each service team has on-call personnel covering a 24/7 schedule. If an incident is assigned a high enough severity, applicable contingency plans are invoked. When a contingency plan is invoked, the incident manager on shift works with the O365 Security team to implement the contingency plan.

Service Infrastructure and Support Systems Change Management

Service- and support-related changes follow an established change management process for the O365 environment. Each change is tracked within identified ticketing systems, which contain information that can be linked to approval and testing details related to the change. These ticketing systems are listed in the Software section above. Appropriate authorizations and approvals needed for the changes being made to these environments are defined in the tickets.

When service teams or customer representatives enter a request for a change to the O365 environment in the change management systems, a representative of the relevant workstream is charged with addressing the change request. If a code modification is required, the addressor will perform a pull request, which replicates the master branch's code and allows the user to perform necessary code modifications without disrupting the live code running in production. Each individual change or addition made to address the change request is subject to a peer review in which another workstream representative reviews and approves the individual code changes. Once a change is peer reviewed and approved, it is checked into a build, along with other changes that are currently in the workstream's deployment process. Each build is subject to security and static analysis testing to test for the presence of security vulnerabilities. Except for in specific scenarios, O365 environment change management processes require 100% testing pass rates prior to moving forward in the deployment process. When a build successfully completes security testing, it is deployed to preproduction environments for integration testing. Builds can be independently deployed to the preproduction environments or multiple builds can be aggregated into a "release," which is subject to integration testing. Code that has successfully completed all testing types is then deployed to the master code repository and is recognized as the newest version of the workstream's source code. There are generally three types of preproduction environments, or "rings," for ring validation integration testing:

- DogFood: The workstream's initial test ring consisting of a subset of Microsoft employees and customers who test changes on Microsoft's behalf.
- MSIT: The MSIT ring allows the release to be subject to testing by all Microsoft employees.
- Slice in Production (SIP): Once the release is successfully integrated into the MSIT ring, it is moved into the SIP environment, which consists of about 5% worldwide customers who have decided to opt in and are able to provide feedback.

Certain types of changes in O365 change management systems are subject to additional review and approval processes dependent on the nature of the change. The four approval levels based on the nature and impact of the change have been included below:

- Auto-approval – A set of preapproved, low-risk standard changes.
- Functional (Peer) Approval – Standard changes with a slightly higher level of risk.
- Change Advisory Board Approval – Changes with the potential for high risk and high impact.
- Emergency Change Advisory Board Approval – A risk that must be remediated timely, such as an out of band security patch.

O365 service teams use a variety of tools to deploy changes to Azure. The ability to deploy code is restricted to appropriate build deployers using a combination of IDM, Torus, and Lockbox permissions.

Security Development Lifecycle

O365 environments follow the standard Microsoft Security Development Lifecycle (SDL) process which includes, at a minimum, risk assessment, testing, approval, and documentation. The SDL process includes security development requirements, which are intended to reduce the number of security-related bugs that appear in the design, code, and documentation associated with a software release, as well as to detect and remove those bugs as early in the SDL as possible.

Risk assessment and design review occurs in a Change Advisory Board entitled “Office Hours” whose members formally “Approve” or “Deny” any major or significant change prior to implementation. Members include representatives from Compliance, Security, OTwC, and Microsoft Legal teams.

Testing, including code reviews, occurs during the development and build processes. Results of the tests, reviews, and approvals are tracked through ticketing systems used by each team. These ticketing systems are listed in the Software section above.

Availability Monitoring

O365 applications and supporting services utilize different tools to monitor and evaluate their service’s health (i.e., capacity, resiliency, and availability). These tools are configured to automatically alert assigned team members of issues impacting service health. For each service team, there are 24x7 On-Call Engineers, or “OCEs”, that monitor and resolve the issues that are reported or identified. Each service utilizes their own custom tools to monitor their respective service’s health. These tools are described in the *Software* section of the report above.

In addition to the above monitoring, O365 senior management reviews capacity, availability, and resiliency reports from the above tools, for anomalies and deviations that could impact availability. On a monthly basis, O365 teams prepare an overview of the service team’s capacity, availability, and resiliency from the prior month. This overview presents the root cause of anomalies or deviations to senior management and based on the meeting issues or changes to capacity and availability are tracked to resolution.

Data Replication and Data Backup

Data for customer content, applications and support services is replicated for redundancy and disaster recovery purposes. O365 applications and supporting services are generally replicated from the primary content database to a secondary content database within the same primary datacenter. The primary and secondary databases are then replicated across geographically dispersed datacenters. Generally, the data maintained in the primary content database is replicated and accessible in real time via: (1) the primary database; (2) a secondary replication database located in the same primary datacenter with real time data; (3) a secondary disaster recovery server with real time replicated data in a geographically segregated datacenter; or (4) a server with a few minutes lag replication in a geographically dispersed datacenter.

In addition to content replication and geographical redundancy, O365 customer content data is also subject to a periodic Azure Blob Storage backup process. Customer content is generally subject to three backup types, each with a unique cadence:

- Full Backups – Full backups consist of all customer content data on a server or content database, generally occur on a weekly frequency and are maintained for 30 days.
- Differential Backups – Differential backups occur at a daily frequency and consist of any additional data since the last full backup or differential backup, depending on which was the last to occur.
- Transaction-Log Backups (“TLog”) – TLog backups occur every 5 minutes and consist of any additional data added in every 5-minute interval.

As data is accessible for redundancy and disaster recovery purposes for applications and support services through the data replication process described above, data backup is performed on applications containing customer content to meet the SLA requirements.

It should be noted that the replication process described above reflects the processes in place for the SfB, EXO, and SPO systems at an overall level. The supporting service teams perform similar replication processes, such as utilizing an Active-Active (e.g., EOP) replication process, but do not maintain lag copies of data. Azure based services rely on Azure capabilities for geo-redundant replication and storage.

Business Continuity

The majority of O365 service teams participate in the Enterprise Business Continuity Management (EBCM) program that uses a common set of criteria to determine the relevancy and frequency of failover exercises. Teams not yet integrated into the EBCM process perform periodic failover testing. Where relevant, failover exercises are conducted on a regular basis to test applications and related data to verify the accessibility at a secondary disaster recovery location. The frequency of conducting failover exercises, as well as the recovery time objectives (RTOs) for each application and support service, are based on the nature and criticality of the systems. The RTOs are developed as part of the overall O365 Business Continuity and Disaster Recovery Planning. The primary objective of conducting failover exercises is to test whether the RTOs may be met in case of a disaster. Issues identified as part of the failover tests are tracked to ultimate resolution.

Customer Termination

Customer content is retained after termination of O365 subscriptions per agreed upon commitments with the customer in the contract and SLAs. Customers are responsible for the upload/download and management of data stored within the O365 environments related to confidentiality.

Processing and Data Integrity

O365 processes data uploaded and managed by the customers per agreed upon processes and procedures. As part of the geographic replication process, data being replicated between datacenters is monitored for completeness and accuracy.

Confidentiality

O365 monitors its dependencies on third parties through obtaining and evaluating attestation reports when available.

Customer content is retained after termination of O365 subscriptions per agreed upon commitments with the customer in the contract and SLAs. Customers are responsible for the upload / download and management of data stored within the O365 environments related to confidentiality.

O365 will remove customer content per contract agreements based on customer account status (e.g., Terminated, Suspended).

Changes During the Examination Period

During the examination period the SfB and Microsoft Teams services started using an internal Microsoft service called IC3. As part of the transition to IC3, the access management processes were brought into scope for the relevant production environments supported by IC3, including the user access review, access provisioning, and access deprovisioning processes.

Trust Criteria and Related Control Activities

Trust criteria mapped to the related control activities is documented in **Section IV** under **Part A**. The testing procedures performed over the related control activities are listed in **Section IV** under **Part B** of this report, “Information Provided by Independent Service Auditor Except for Trust Services Criteria and Control Activities,” to reduce the redundancy that would result from listing them in this section and repeating them in **Section IV**. While these controls are listed in **Section IV**, the service organization remains responsible for the representations in the description of controls. These control activities include preventive, detective, and corrective policies and procedures that help O365 identify, decrease, manage, and respond to risk in a timely manner.

Principal Service Commitments and System Requirements

Microsoft makes service commitments to its customers and has established system requirements as part of the O365 service. Some of these commitments are principal to the performance of the service and relate to applicable trust services criteria. O365 is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that O365’s service commitments and system requirements are achieved.

Service commitments to customers are documented and communicated in [Service Level Agreements](#) (SLAs) and other customer agreements such as the [Microsoft Online Service Terms](#), [Microsoft Product Licensing](#), [Microsoft Privacy Statement](#), and [Microsoft Trust Center](#), as well as in the description of the service offering provided online. Service commitments include, but are not limited to, the following:

- **Security:** O365 has made commitments related to securing customer data and complying with relevant laws and regulations. These commitments are addressed through measures including data encryption, authentication mechanisms, physical security and other relevant security controls.
- **Availability:** O365 has made commitments related to percentage uptime and connectivity for Azure as well as commitments related to service credits for instances of downtime.
- **Processing Integrity:** O365 has made commitments related to processing customer actions completely, accurately and timely. These customer actions include, for example, specifying geographic regions for the storage and processing of customer data.
- **Confidentiality:** O365 has made commitments related to maintaining the confidentiality of customers’ data through data classification policies, data encryption and other relevant security controls.

Microsoft has established operational requirements that support the achievement of service commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in O365’s system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of various O365 services.

Complementary User Entity Control Considerations (CUECs)

Microsoft O365 transaction processing and the controls over that processing were designed with the assumption that certain controls are in operation within the user entity organizations. This section describes those controls that should be in operation at user entity organizations to complement the controls of O365. The following list contains controls that O365 assumes their user entities have implemented. User organization auditors should determine whether the user entities have established sufficient controls in these areas:

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-01: User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.	CC6.1, CC6.2, CC6.3, CC6.6
CUEC-02: User entities establish proper controls over the use of system IDs and passwords.	CC6.6
CUEC-03: User entities are responsible for managing their user's password authentication mechanism.	CC6.6
CUEC-04: User entities enforce desired level of encryption for network sessions.	CC6.1, CC6.7, C1.1
CUEC-05: User entities manage anonymous access to SPO and SfB sessions.	CC6.1
CUEC-06: User entities secure the software and hardware used to access O365.	CC6.1, CC6.3, CC6.6, CC6.7, CC6.8, CC7.1, A1.2
CUEC-07: User entities conduct end-user training.	CC7.2, CC9.2
CUEC-08: User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.	CC3.2, CC7.2, CC7.3, CC7.4, CC7.5, CC9.2, PI1.1
CUEC-09: User entities are responsible for enabling and maintaining email restoration for EXO.	CC9.1, A1.2, A1.3
CUEC-10: User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.	CC2.3, CC6.5, CC6.7, CC7.5, PI1.1, PI1.5
CUEC-11: User entities are responsible for managing their data inputs, and data uploads to O365 for completeness, accuracy, and timeliness.	PI1.2
CUEC-12: User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.	PI1.1, PI1.2, PI1.3
CUEC-13: User entities are responsible for managing their stored data for completeness and accuracy.	PI1.5
CUEC-14: User entities are responsible for managing their data output from O365 for completeness, accuracy, and timeliness.	PI1.4
CUEC-15: When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner.	CC6.1

Complementary User Entity Controls	Relevant SOC 2 Control Criteria
CUEC-16: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys.	CC6.7, C1.1
CUEC-17: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription.	CC6.7, C1.1
CUEC-18: User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.	CC6.7, C1.1

Complementary Subservice Organization Controls (CSOCs)

Microsoft's controls related to the O365 system detailed in this report cover only a portion of overall internal control for each user entity of O365. It is not feasible for the control criteria related to O365 to be achieved solely by Microsoft. Therefore, in conjunction with O365's controls, a user entity must take into account the related complementary subservice organization controls expected to be implemented at the subservice organizations as follows. Note that the CSOCs associated with the subservice organizations are summarized in the table below, refer to the **Section IV** control mapping for more on the specific CSOCs associated with the criteria.

Type of Services Provided	Subservice Organization Name	Complementary Subservice Organization Controls	Relevant SOC 2 Control Criteria
Platform as a Service/Infrastructure as a Service	Microsoft Azure	<p>Microsoft Azure is responsible for maintaining controls over access management (including authentication), change management, operational controls, and data protection to the platform services supporting O365.</p> <p>Additionally, for services using Azure, Azure is responsible for maintaining controls over:</p> <ul style="list-style-type: none"> secure transmission, handling, and storage of data (including encryption, backups, replication, and recovery). security, incident, and vulnerability management. 	CC6.1, CC6.2, CC6.3, CC6.5, CC6.6, CC6.7, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1, PI1.5
Infrastructure as a Service	Microsoft Datacenters	<p>Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities supporting O365, including datacenters.</p> <p>Additionally, Microsoft Datacenters is responsible for maintaining controls over:</p> <ul style="list-style-type: none"> environmental threats (including natural disasters and man-made threats). the protection of network equipment (including firewalls and other devices). security, incident, and vulnerability management. 	CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC7.1, CC7.2, CC7.3, CC7.4, CC7.5, CC9.1, A1.2, A1.3, C1.1, PI1.5

Section IV:

Information Provided by Independent Service Auditor, Except for Trust Services Criteria and Control Activities

Introduction

This report, including the description of tests of controls and results thereof in this section, is intended solely for the information and use of Microsoft Corporation (“Microsoft”), user entities of Microsoft’s system related to related to its Microsoft Office 365, including Office 365 with International Traffic in Arms Regulations (ITAR)⁴ Support, online services (“O365”), during some or all of the period October 1, 2020, through September 30, 2021, business partners of Microsoft subject to risks arising from interactions with Microsoft’s system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following: the nature of the service provided by the service organization; how the service organization’s system interacts with user entities, subservice organizations, and other parties; internal control and its limitations; complementary user-entity controls and how they interact with related controls at the service organization to meet the applicable trust services criteria; the applicable trust services criteria; and the risks that may threaten the achievement of the applicable trust services criteria and how controls address those risks.

- The controls established and specified by Microsoft to achieve the specified trust services criteria.

Also included in this section is the following information provided by Deloitte & Touche LLP:

- A description of the tests performed by Deloitte & Touche LLP to determine whether Microsoft’s controls were operating with sufficient effectiveness to achieve specified trust services criteria. Deloitte & Touche LLP determined the nature, timing, and extent of the testing performed.
- The results of Deloitte & Touche LLP’s tests of controls.

The examination was conducted in accordance with the criteria as set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization’s System in a SOC 2® Report* (“description criteria”) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period October 1, 2020, to September 30, 2021, to provide reasonable assurance that Microsoft’s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (“applicable trust services criteria”) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, of the American Institute of Certified Public Accountants (AICPA), and the AICPA Statement on Standards for Attestation Engagements No. 18 (SSAE 18) and International Standard on Assurance Engagements 3000, *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. SSAE 18 is inclusive of the following: (1) AT-C 105, Concepts Common to all Attestation Engagements; and (2) AT-C 205, Examination Engagements. Our testing of Microsoft’s controls was restricted to the controls identified by Microsoft to meet the criteria related to security, availability, processing integrity, and confidentiality listed in **Section IV** of this report and was not extended to controls described in

⁴ This report is a description of the “Microsoft Office 365 with ITAR Support system” (O365) as defined in the system description. The inclusion of the ITAR reference in the formal name of the system is not intended to examine or opine on the requirements of the United States International Traffic in Arms Regulations (ITAR).

Section III but not included in **Section IV**, or to controls that may be in effect at user organizations or subservice organizations.

It is each user's responsibility to evaluate the information included in this report in relation to internal control in place at individual user entities and subservice organizations to obtain an understanding and to assess control risk at the user entities. The controls at user entities, subservice organizations, and Microsoft's controls should be evaluated together. If effective user entity or subservice organizations controls are not in place, Microsoft's controls may not compensate for such weaknesses.

Control Environment Elements

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for other components of internal control, providing discipline and structure. In addition to the tests of design, implementation, and operating effectiveness of controls identified by Microsoft, our procedures included tests of the following relevant elements of Microsoft's control environment:

- | | |
|---------------------------------|----------------------------------|
| a. Integrity and Ethical Values | e. OLC, IA Department, AC |
| b. Microsoft SBC | f. Risk Assessment |
| c. Training and Accountability | g. Information and Communication |
| d. Commitment to Competence | h. Monitoring |

Such tests included inquiry of the appropriate management, supervisory, and staff personnel; observation of Microsoft's activities and operations, inspection of Microsoft's documents and records, and reperformance of the application of Microsoft's controls. The results of these tests were considered in planning the nature, timing, and extent of our testing of the control activities described in this section.

Tests of Operating Effectiveness

Our tests of the controls were designed to cover a representative number of transactions throughout the period from October 1, 2020, through September 30, 2021. In determining the nature, timing, and extent of tests, we considered, (a) the nature and frequency of the controls being tested, (b) the types of available evidential matter, (c) the nature of the trust services criteria to be met, (d) the assessed level of control risk, (e) the expected effectiveness of the test, and (f) the results of our tests of the control environment.

Description of Testing Procedures Performed

Deloitte & Touche LLP performed a variety of tests relating to the controls listed in this section throughout the period from October 1, 2020, through September 30, 2021. Our tests of controls were performed on controls as they existed during the period of October 1, 2020, through September 30, 2021, and were applied to those controls relating to the trust services criteria.

In addition to the tests listed below, ascertained through multiple inquiries with management and the control owner that each control activity listed below operated as described throughout the period. Tests performed are described below:

Test	Description
Corroborative inquiry	Conducted detailed interviews with relevant personnel to obtain evidence that the control was in operation during the report period and is accompanied by other procedures noted below that are necessary to corroborate the information derived from the inquiry.
Observation	Observed the performance of the control during the reporting period to evidence application of the specific control activity.

Test	Description
Examination of documentation/inspection	If the performance of the control is documented, inspected documents and reports indicating performance of the control.
Reperformance of monitoring activities or manual controls	Obtained documents used in the monitoring activity or manual control activity and independently reperfomed the procedures. Compared any exception items identified with those identified by the responsible control owner.

Reliability of Information Produced by the Service Organization

We performed procedures to evaluate whether the information provided by the service organization, which includes (a) information provided by the service organization to the service auditor in response to ad hoc requests from the service auditor (e.g., population lists); (b) information used in the execution of a control (e.g., exception reports or transaction reconciliations); and (c) information prepared for user entities (e.g., user access lists), was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes. Information we utilized as evidence may have included, but was not limited to:

- Standard “out of the box” reports as configured within the system
- Parameter-driven reports generated by Microsoft’s systems
- Custom-developed reports that are not standard to the application such as scripts, report writers, and queries
- Spreadsheets that include relevant information utilized for the performance or testing of a control
- Microsoft prepared analyses, schedules, or other evidence manually prepared and utilized by Microsoft

Our procedures to evaluate whether this information was sufficiently reliable included obtaining evidence regarding the accuracy and completeness included procedures to address (a) the accuracy and completeness of source data and (b) the creation and modification of applicable report logic and parameters. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information is sufficiently precise and detailed for purposes of fully testing the controls identified by Microsoft.

Reporting on Results of Testing

The concept of materiality is not applied when reporting the results of tests of controls for which deviations have been identified because Deloitte & Touche LLP does not have the ability to determine whether a deviation will be relevant to a particular user entity. Consequently, Deloitte & Touche LLP reports all deviations.

Description of Control Activities

The information regarding the tests of operating effectiveness is explained below in two parts:

- **Part A:** Contains the Trust Services Criteria, and the related O365 control activities that cover those criteria.
- **Part B:** Contains the details of the test procedures performed to test the operating effectiveness of the O365 control activities and the results of the testing.

The Security, Availability, Processing Integrity, and Confidentiality Trust Services Criteria and O365 Control Activities in **Part A** and **Part B** are provided by Microsoft.

Note: In Part B, there are certain gaps in control activity numbering as a result of updates to the control environment and supporting policies and procedures. Thus, the following control numbers are intentionally omitted: CA-28, CA-42, CA-52, ELC-05, ELC-13, and ELC-14.

Part A: Trust Services Criteria and O365 Control Activities provided by Microsoft

Criteria Common to All Security, Availability, Processing Integrity, and Confidentiality Principles

CC1.0 – Common Criteria Related to the Control Environment

Criteria	Office 365 Control Activity
CC1.1 – COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<p>CA-04 – Employees hold periodic “connects” with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p> <p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>ELC-01 – Microsoft’s values are accessible to employees via the Values SharePoint site and are updated as necessary by management.</p> <p>ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p>

Criteria	Office 365 Control Activity
<p>CC1.2 – COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.</p>	<p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>ELC-03 – The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>
<p>CC1.3 – COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>

Criteria	Office 365 Control Activity
<p>CC1.4 – COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objective.</p>	<p>CA-04 – Employees hold periodic “connects” with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p> <p>CA-06 – The Candidates job descriptions are created and documented for open positions within O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities.</p> <p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-08 – The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>ELC-01 – Microsoft’s values are accessible to employees via the Values SharePoint site and are updated as necessary by management.</p> <p>ELC-06 – The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.</p>

Criteria	Office 365 Control Activity
<p>CC1.5 – COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-04 – Employees hold periodic “connects” with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p> <p>CA-06 – The Candidates job descriptions are created and documented for open positions within O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities.</p> <p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p>

CC2.0 – Common Criteria Related to Communication and Information

Criteria	Office 365 Control Activity
CC2.1 – COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.</p> <p>CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>

Criteria	Office 365 Control Activity
<p>CC2.2 – COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment</p> <p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p>CA-16 – Customers can report issues and potential incidents by creating a service request through the admin portal, which includes the option for telephone support. Service request status and activity can be viewed through the Admin Center.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system</p> <p>ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p>

Criteria	Office 365 Control Activity
<p>CC2.3 – COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.</p>	<p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-10 – Office 365 provides customers and external users self-service with compliance reporting related to Office 365's services and systems within the Service Trust Portal website. In addition to compliance reporting, the Service Trust Portal details the customer's and external user's responsibilities for service and system operation.</p> <p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p>CA-14 – Changes and updates to the Office 365 environment are communicated through the Message Center which is part of the Office 365 Admin Center.</p> <p>CA-15 – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center.</p> <p>CA-16 – Customers can report issues and potential incidents by creating a service request through the admin portal, which includes the option for telephone support. Service request status and activity can be viewed through the Admin Center.</p>

Criteria	Office 365 Control Activity
<p>CC2.3 – COSO Principle 15 (continued): The entity communicates with external parties regarding matters affecting the functioning of internal control.</p>	<p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p>CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.</p> <p>ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.</p> <p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.</p>

CC3.0 – Common Criteria Related to Risk Assessment

Criteria	Office 365 Control Activity
<p>CC3.1 – COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.</p> <p>CA-09 – Office 365 system information regarding the design and operation of its services is available to users online through Microsoft web portals.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>

Criteria	Office 365 Control Activity
<p>CC3.1 – COSO Principle 6 (continued): The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.</p>	<p>ELC-12 – Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in the Statement of Work template. Including understanding the consequences of violating relevant laws, regulations, provisions, and policies regarding information security.</p> <p>ELC-15 – Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Office 365 environment based on Microsoft’s corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p>
<p>CC3.2 – COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</p>	<p>CA-13 – Incident response guides are used by Office 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p>

Criteria	Office 365 Control Activity
<p>CC3.2 – COSO Principle 7 (continued): The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.</p>	<p>CA-27 – There is a continual process for host vulnerability scanning, reporting, and management review within the Office 365 environment. Individual or centralized service teams apply patches and remediate vulnerabilities, which are verified and reported to management through a common process. Responses are tracked for both compliant and non-compliant hosts to identify any outstanding vulnerabilities that need to be addressed by the service teams.</p> <p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>ELC-09 – Microsoft’s Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.</p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p>

Criteria	Office 365 Control Activity
<p>CC3.3 – COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.</p>	<p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>

Criteria	Office 365 Control Activity
<p>CC3.4 – COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.</p>	<p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-06 – The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>

CC4.0 – Common Criteria Related to Monitoring Activities

Criteria	Office 365 Control Activity
<p>CC4.1 – COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>ELC-11 – Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. Audit findings are addressed relative to their criticality.</p>

Criteria	Office 365 Control Activity
<p>CC4.2 – COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.</p>	<p>CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-15 – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p> <p>ELC-11 – Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. Audit findings are addressed relative to their criticality.</p>

CC5.0 – Common Criteria Related to Control Activities

Criteria	Office 365 Control Activity
<p>CC5.1 – COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>ELC-10 – Teams evaluate changes according to criteria defined by GRC. Changes that meet the criteria go through a review that includes a risk assessment.</p>

Criteria	Office 365 Control Activity
<p>CC5.2 – COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p> <p>ELC-10 – Teams evaluate changes according to criteria defined by GRC. Changes that meet the criteria go through a review that includes a risk assessment.</p>

Criteria	Office 365 Control Activity
<p>CC5.3 – COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft’s continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p> <p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

Criteria	Office 365 Control Activity
CC6.1 – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.	<p>CA-08 – The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.</p> <p>CA-32 – Access to shared accounts within the Office 365 environment are restricted to authorized personnel.</p> <p>CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.</p> <p>CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.</p> <p>CA-34 – Identity of users is authenticated to Office 365 Services. The use of passwords incorporates policy on periodic change and password complexity.</p> <p>CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.</p> <p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p>CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>CA-37 – Each Office 365 Service customer’s content is segregated either logically or physically from other Online Services customers’ content.</p> <p>CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.</p> <p>CA-40 – Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.</p> <p>CA-41 – Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms.</p> <p>CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.</p> <p>CA-57 – Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.</p>

Criteria	Office 365 Control Activity
<p>CC6.1 (continued) – The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.</p>	<p>CA-58 – Customer Lockbox elevation requests to customer content require an associated service request.</p>
	<p>CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.</p>
	<p>CA-60 – The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.</p>
	<p>CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.</p>
	<p>CA-64 – Only keys noted in the tenant’s Data Encryption Policy can be used to access the data maintained in that tenant’s service encryption.</p>
	<p>CA-65 – Customer content resides in a specific geographic location.</p>
	<p><i>Complementary Subservice Organization Controls</i></p>
	<p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.</p>
	<p><i>Complementary User Entity Controls</i></p>
	<p>CUEC-01 – User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.</p>
	<p>CUEC-04 – User entities enforce desired level of encryption for network sessions.</p>
	<p>CUEC-05 – User entities manage anonymous access to SPO and SfB sessions.</p>
	<p>CUEC-06 – User entities secure the software and hardware used to access O365.</p>
	<p>CUEC-15 – When employing Customer Lockbox, user entities are responsible for reviewing Microsoft requests to customer content and approving appropriate requests in a timely manner.</p>

Criteria	Office 365 Control Activity
<p>CC6.2 – Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</p>	<p>CA-08 – The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.</p> <p>CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.</p> <p>CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.</p> <p>CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.</p> <p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p>CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.</p> <p>CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-01 – User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.</p>

Criteria	Office 365 Control Activity
<p>CC6.3 – The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.</p>	<p>CA-08 – The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.</p> <p>CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.</p> <p>CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.</p> <p>CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.</p> <p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p>CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.</p> <p>CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-01 – User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.</p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p>

Criteria	Office 365 Control Activity
<p>CC6.4 – The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.</p>	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 that address environmental threats including natural disasters and man-made threats.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.</p> <p>CSOC - Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting O365.</p>
<p>CC6.5 – The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.</p>	<p>CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.</p>

Criteria	Office 365 Control Activity
<p>CC6.6 – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p>	<p>CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.</p> <p>CA-32 – Access to shared accounts within the Office 365 environment are restricted to authorized personnel.</p> <p>CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.</p> <p>CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.</p> <p>CA-34 – Identity of users is authenticated to Office 365 Services. The use of passwords incorporates policy on periodic change and password complexity.</p> <p>CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.</p> <p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p>CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.</p> <p>CA-40 – Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.</p> <p>CA-41 – Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms.</p> <p>CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.</p> <p>CA-57 – Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.</p> <p>CA-58 – Customer Lockbox elevation requests to customer content require an associated service request.</p> <p>CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.</p> <p>CA-60 – The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.</p>

Criteria	Office 365 Control Activity
<p>CC6.6 (continued) – The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</p>	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over authentication and logical access, including account provisioning and deprovisioning, to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-01 – User entities properly authorize users who are granted access to the resources and monitor continued appropriateness of access.</p> <p>CUEC-02 – User entities establish proper controls over the use of system IDs and passwords.</p> <p>CUEC-03 – User entities are responsible for managing their user’s password authentication mechanism.</p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p>
<p>CC6.7 – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.</p>	<p>CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.</p> <p>CA-37 – Each Office 365 Service customer’s content is segregated either logically or physically from other Online Services customers’ content.</p> <p>CA-44 – Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.</p> <p>CA-45 – Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available.</p> <p>CA-54 – Data at rest is encrypted per policy.</p> <p>CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.</p> <p>CA-62 – Customer mailboxes are encrypted per customer’s defined encryption policies using keys generated and maintained by the customer.</p> <p>CA-63 – When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.</p> <p>CA-64 – Only keys noted in the tenant’s Data Encryption Policy can be used to access the data maintained in that tenant’s service encryption.</p>

Criteria	Office 365 Control Activity
<p>CC6.7 (continued) – The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.</p>	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data protection for data at rest and in motion to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including perimeter firewalls and restricting access to network devices.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-04 – User entities enforce desired level of encryption for network sessions.</p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality</p> <p>CUEC-16 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys.</p> <p>CUEC-17 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription.</p> <p>CUEC-18 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.</p>

Criteria	Office 365 Control Activity
<p>CC6.8 – The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity’s objectives.</p>	<p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p> <p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p> <p>CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server’s intended use.</p> <p>CA-45 – Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available.</p> <p>CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p>CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.</p>
	<p><i>Complementary User Entity Controls</i></p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p>

CC7.0 – Common Criteria Related to Systems Operations

Criteria	Office 365 Control Activity
<p>CC7.1 – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.</p> <p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p> <p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p> <p>CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server’s intended use.</p> <p>CA-45 – Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available.</p> <p>CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p>CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.</p> <p>Complementary Subservice Organization Controls</p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for O365 services hosted on the Azure platform.</p>

Criteria	Office 365 Control Activity
<p>CC7.1 (continued) – To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</p>	<p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p>
<p>CC7.2 – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p>	<p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p> <p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p> <p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p> <p>CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server's intended use.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p>CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.</p>

Criteria	Office 365 Control Activity
<p>CC7.2 (continued) – The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.</p>	<p>CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines.</p> <p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for O365 services hosted on the Azure platform.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-07 – User entities conduct end-user training.</p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p>
<p>CC7.3 – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p>	<p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p> <p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p> <p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p>

Criteria	Office 365 Control Activity
<p>CC7.3 (continued) – The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.</p>	<p>CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server’s intended use.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for O365 services hosted on the Azure platform.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p>
<p>CC7.4 – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-13 – Incident response guides are used by Office 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p>

Criteria	Office 365 Control Activity
<p>CC7.4 (continued) – The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate</p>	<p>CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.</p> <p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p> <p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for O365 services hosted on the Azure platform.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p>

Criteria	Office 365 Control Activity
<p>CC7.5 – The entity identifies, develops, and implements activities to recover from identified security incidents.</p>	<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p> <p>CA-13 – Incident response guides are used by Office 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed.</p> <p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p> <p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p> <p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p> <p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.</p> <p>CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.</p> <p>ELC-09 – Microsoft’s Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.</p>

Criteria	Office 365 Control Activity
<p>CC7.5 (continued) – The entity identifies, develops, and implements activities to recover from identified security incidents.</p>	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over security and incident management, including incident identification and remediation, server vulnerability scanning, and patch management for O365 services hosted on the Azure platform.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over protection of the network environment, including configuration management, incident management, and vulnerability scanning and remediation.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.</p>

CC8.0 – Common Criteria Related to Change Management

Criteria	Office 365 Control Activity
CC8.1 – The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	<p>CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.</p> <p>CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.</p> <p>CA-14 – Changes and updates to the O365 environment are communicated through the admin Message Center part of the O365 Admin Center.</p> <p>CA-18 – Changes and software releases within the Office 365 environment are documented / tracked and are approved prior to implementation into production.</p> <p>CA-19 – For teams utilizing the Developer / Operations model, monitoring processes or system configurations are in place to identify and remediate unapproved changes to production.</p> <p>CA-20 – Emergency changes to the production environment follow an emergency change approval process.</p> <p>CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.</p> <p>CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.</p>

CC9.0 – Common Criteria Related to Risk Mitigation

Criteria	Office 365 Control Activity
CC9.1 – The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines</p> <p>CA-51 – Customer content and services are replicated to a geographically separate location.</p> <p>ELC-09 – Microsoft’s Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including data centers, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 that address environmental threats including natural disasters and man-made threats.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-09 – User entities are responsible for enabling and maintaining email restoration for EXO.</p>

Criteria	Office 365 Control Activity
<p>CC9.2 – The entity assesses and manages risks associated with vendors and business partners</p>	<p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p> <p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p> <p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p> <p>CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.</p> <p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft’s Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p> <p>ELC-12 – Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in the Statement of Work template. Including understanding the consequences of violating relevant laws, regulations, provisions, and policies regarding information security.</p> <p>ELC-15 – Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Office 365 environment based on Microsoft’s corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-07 – User entities conduct end-user training.</p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p>

Additional Criteria for Availability

Criteria	Office 365 Control Activity
<p>A1.1 – The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.</p>	<p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p> <p>CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.</p> <p>CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.</p>

Criteria	Office 365 Control Activity
<p>A1.2 – The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.</p>	<p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p> <p>CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.</p> <p>CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines.</p> <p>CA-51 – Customer content and services are replicated to a geographically separate location.</p> <p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 that address environmental threats including natural disasters and man-made threats.</p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting O365.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-06 – User entities secure the software and hardware used to access O365.</p> <p>CUEC-09 – User entities are responsible for enabling and maintaining email restoration for EXO.</p>

Criteria	Office 365 Control Activity
<p>A1.3 – The entity tests recovery plan procedures supporting system recovery to meet its objectives.</p>	<p>CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.</p> <p>CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full datacenter failover), and remediation timelines.</p> <p>CA-51 – Customer content and services are replicated to a geographically separate location.</p>
	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical access to the facilities, including datacenters, supporting O365. Additionally, Microsoft Datacenters is responsible for maintaining controls for O365 that address environmental threats including natural disasters and man-made threats.</p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data replication and redundancy to the platform services supporting O365.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-09 – User entities are responsible for enabling and maintaining email restoration for EXO.</p>

Additional Criteria for Processing Integrity

Criteria	Office 365 Control Activity
<p>PI1.1 – The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p>CA-66 – Production data is classified and protected based upon the Office 365 data classification process.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-08 – User entities are responsible for reporting any identified security, availability, processing integrity, and confidentiality issues.</p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.</p> <p>CUEC-12 – User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.</p>
<p>PI1.2 – The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.</p>	<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p> <p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-11 – User entities are responsible for managing their data inputs, and data uploads to O365 for completeness, accuracy, and timeliness.</p> <p>CUEC-12 – User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.</p>

Criteria	Office 365 Control Activity
<p>PI1.3 – The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity’s objectives.</p>	<p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p> <p>CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.</p> <p>CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.</p> <p>CA-51 – Customer content and services are replicated to a geographically separate location.</p> <p>CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.</p> <p>CA-57 – Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.</p>
	<p><i>Complementary User Entity Controls</i></p>
	<p>CUEC-12 – User entities are responsible for managing their data processing within O365 for completeness, accuracy, and timeliness.</p>

Criteria	Office 365 Control Activity
<p>PI1.4 – The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity’s objectives.</p>	<p>CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.</p> <p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p> <p>CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.</p> <p>CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.</p> <p>CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-14 – User entities are responsible for managing their data output from O365 for completeness, accuracy, and timeliness.</p>

Criteria	Office 365 Control Activity
<p>PI1.5 – System output is complete, accurate, distributed, and retained to meet the entity’s processing integrity commitments and system requirements.</p>	<p>CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.</p> <p>CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.</p> <p>CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.</p> <p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p>CA-51 – Customer content and services are replicated to a geographically separate location.</p> <p>CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.</p> <p>CA-60 – The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.</p> <p>CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.</p> <p>CA-65 – Customer content resides in a specific geographic location.</p>
	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data protection for data at rest and in motion to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting O365.</p>
	<p><i>Complementary User Entity Controls</i></p> <p>CUEC-10 – User entities are responsible for understanding and adhering to the contents of their service contracts, including commitments related to system security, availability, processing integrity, and confidentiality.</p> <p>CUEC-13 – User entities are responsible for managing their stored data for completeness and accuracy.</p>

Additional Criteria for Confidentiality

Criteria	Office 365 Control Activity
<p>C1.1 – The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.</p>	<p>CA-40 – Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.</p> <p>CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner.</p> <p>CA-44 – Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.</p> <p>CA-54 – Data at rest is encrypted per policy</p> <p>CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.</p> <p>CA-62 – Customer mailboxes are encrypted per customer’s defined encryption policies using keys generated and maintained by the customer.</p> <p>CA-63 – When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.</p> <p>CA-64 – Only keys noted in the tenant’s Data Encryption Policy can be used to access the data maintained in that tenant’s service encryption.</p> <p>CA-65 – Customer content resides in a specific geographic location.</p> <p>CA-66 – Production data is classified and protected based upon the Office 365 data classification process.</p>

Criteria	Office 365 Control Activity
<p>C1.1 (continued) – The entity identifies and maintains confidential information to meet the entity’s objectives related to confidentiality.</p>	<p><i>Complementary Subservice Organization Controls</i></p> <p>CSOC – Microsoft Azure – Microsoft Azure is responsible for maintaining controls over data protection for data at rest and in motion to the platform services supporting O365.</p> <p>CSOC – Microsoft Datacenters – Microsoft Datacenters is responsible for maintaining controls over physical data storage, protection, and disposal services supporting O365.</p> <p><i>Complementary User Entity Controls</i></p> <p>CUEC-04 – User entities enforce desired level of encryption for network sessions.</p> <p>CUEC-16 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for importing or generating their own encryption keys.</p> <p>CUEC-17 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for restricting access to the Azure Key Vault subscription.</p> <p>CUEC-18 – User entities subscribing to Storage Service Encryption with Customer Managed Keys are responsible for rotating customer managed keys per their compliance policies.</p>
<p>C1.2 – The entity disposes of confidential information to meet the entity’s objectives related to confidentiality.</p>	<p>CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.</p> <p>CA-63 – When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.</p> <p>CA-66 – Production data is classified and protected based upon the Office 365 data classification process.</p>

Part B: Microsoft O365 Control Activities Provided by Microsoft and Test Results Provided by Deloitte & Touche LLP

Control Activity	Tests Performed	Test Result
<p>CA-01 – An Office 365 security team has been defined and is responsible for Security issues within the Office 365 environment. Service teams have operations personnel who are responsible for system operation and service availability.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that a defined O365 Security team has been established and that the team's responsibilities include management of security, availability, confidentiality, and processing integrity issues within the O365 environment. • Obtained and inspected an organizational chart demonstrating the existence of a dedicated O365 Security team. • Obtained meeting minutes and policy documentation to ascertain that responsibilities for O365 Security personnel are defined and include the management of security, system operation, and service availability issues in the O365 environment, as well as the design, development, implementation, and maintenance of security, availability, processing integrity, and confidentiality during SDLC changes. 	No Exceptions Noted
<p>CA-02 – An Office 365 Governance, Risk, and Compliance team has been defined and is responsible for Security, Availability, Confidentiality, and Processing Integrity controls within the Office 365 environment.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that a defined O365 Governance, Risk, and Compliance team has been established and that the team is responsible for overseeing security, availability, confidentiality, and processing integrity controls within the O365 environment. • Obtained and inspected an organizational chart demonstrating the existence of a dedicated O365 Governance, Risk & Compliance team. • Obtained policy documentation to ascertain that responsibilities for O365 Governance, Risk & Compliance personnel are defined and include the management of O365 security, availability, confidentiality, and processing integrity controls. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-03 – Senior Management, as part of its major system release planning process, considers its commitments and requirements for Security, Availability, Confidentiality, and Processing Integrity.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that Senior Management considers its commitments and requirements related to security, availability, confidentiality, and processing integrity as part of its major system release planning process. • Obtained and inspected a sample selection of evidence including memorandums and planning meeting records, to ascertain that commitments and requirements for security, availability, confidentiality, and processing integrity were considered and approved by Senior Management, and these commitments and requirements were communicated to relevant personnel as part of the major system release planning process. 	No Exceptions Noted
<p>CA-04 – Employees hold periodic “connects” with their managers to validate they are on the expected Career Path and facilitate greater collaboration. They also review their performance against their documented deliverables (priorities) and discuss the results with their managers.</p>	<ul style="list-style-type: none"> • Inquired of HR process owners to ascertain that performance reviews take place where employee commitments are evaluated by his/her manager on a semi-annual basis. • Obtained and inspected extracts from the Connect tool for a selection of employees to ascertain that they completed a performance evaluation annually. • Obtained and inspected extracts from the Connect tool to ascertain that a sample performance review includes an evaluation of employee performance against their assigned priorities. 	No Exceptions Noted
<p>CA-05 – The Governance, Risk, and Compliance team updates the data flow diagrams and service offerings of O365 with the individuals that act as point of contact for each service offering.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that O365 data flow diagrams and service offering point of contacts are reviewed and updated on a semi-annual basis. • Obtained and inspected evidence for a sample of data flow diagram updates to ascertain that the GRC team reviews the service offering data flow diagrams with the point of contacts and that they update the data flow diagrams accordingly. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-06 – The Candidates job descriptions are created and documented for open positions within O365. Job descriptions include desired candidate competencies and expected job roles and responsibilities.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk, & Compliance process owners to ascertain that candidate's job descriptions are created and documented for open positions within O365. • Obtained and inspected a sample job posting to ascertain that the job listing includes desired candidate competencies and expected job roles and responsibilities. 	No Exceptions Noted
<p>CA-07 – Microsoft Office of Legal Compliance (OLC) updates the Standards of Business Conduct as necessary and the Code is made available to all employees through an internal Microsoft site. The SBC reflects Microsoft's continued commitment to ethical business practices and regulatory compliance. Periodically, the OLC releases a Standards of Business Conduct training course that is mandatory for all employees. Employees who do not complete the training on time are tracked and followed up with appropriately.</p>	<ul style="list-style-type: none"> • Inquired of HR process owners to ascertain that a defined Standards of Business Conduct policy was established and is communicated to Office 365 personnel through intranet sites and trainings. • Obtained and inspected the Standards of Business Conduct to ascertain that the standards include Microsoft's continued commitment to security, availability, confidentiality, and processing integrity, and also, ethical business practices and regulatory compliance. • Obtained and inspected course completion status for a selection of employees to ascertain that the Standard of Business Conduct training course has been completed. 	No Exceptions Noted
<p>CA-08 – The Microsoft Office 365 Service group works with Microsoft Human Resources and vendor companies to perform a background check on new or transferred personnel worldwide, where permitted by law before they are granted access to the Microsoft Office 365 production assets containing customer content.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance (GRC) process owners that new and transferred applicable employees and contractors are required to undergo a background check prior to being granted access to the environment. • Obtained and inspected background check data for a selection of Microsoft personnel to ascertain that a background check was performed prior to granting access to the production assets containing customer content. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-09 – Office 365 system information regarding the design and operation of its services is available to users online through Microsoft web portals.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that O365 system design and operation information is accessible to employees. Observed the Microsoft web portals to ascertain that design and operation information for the O365 system is available and accessible to users. 	No Exceptions Noted
CA-10 – Office 365 provides customers and external users self-service with compliance reporting related to Office 365's services and systems within the Service Trust Portal website. In addition to compliance reporting, the Service Trust Portal details the customer's and external user's responsibilities for service and system operation.	<ul style="list-style-type: none"> Inquired of Governance, Risk, & Compliance process owners to ascertain that customers can obtain the SOC report for O365 through the Service Trust Portal. Observed the Service Trust Portal to ascertain that the O365 SOC report and its associated CUECs is available to customers. 	No Exceptions Noted
CA-11 – On an annual basis services are updated to reflect changes made to the Office 365 control framework.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that the O365 control framework is reviewed and updated on an annual basis by service teams. Obtained and inspected documentation from various ticketing systems to ascertain that service teams reviewed the O365 Control Framework with the point of contacts and updated the framework accordingly. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-12 – Office 365 communicates its commitments to customers in SLAs. These commitments are reflected in the control framework, which defines regulatory, security, availability, confidentiality, and processing integrity requirements. This information is distributed internally through policies, training, and Office Hours.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that O365 communicates its regulatory, security, availability, confidentiality, and processing integrity commitments to customers using SLAs, and that these commitments are also distributed internally. Obtained and inspected policy and communication documentation to ascertain that SLAs defining regulatory, security, availability, confidentiality, and processing integrity commitments are distributed to O365 customers. Obtained and inspected policy and communication documentation to ascertain that regulatory, security, availability, confidentiality, and processing integrity requirements are distributed internally through methods including trainings, policies, and Office Hours. 	No Exceptions Noted
CA-13 – Incident response guides are used by Office 365 personnel for the handling and reporting of security incidents. These guides are stored on internal SharePoint sites and are updated as needed.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that incident response guides, which provide guidance on management and reporting of security incidents, are accessible to O365 personnel on internal SharePoint sites. Obtained and inspected the O365 incident response guides to ascertain that they are available to personnel on the intranet and outline procedures to be followed for handling and reporting of security incidents. 	No Exceptions Noted
CA-14 – Changes and updates to the O365 environment are communicated through the admin Message Center part of the O365 Admin Center.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that incidents and changes to the O365 environment are made available to customers using the Customer Portal. Obtained and inspected newsletters for a sample customer to ascertain that monthly newsletters containing O365 incident and change information are available on the Customer Portal. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-15 – Service impacting incidents, including security incidents, are communicated to the customer through the Service Health Center.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that information related to security, availability, confidentiality, and processing integrity issues can be reported and received using the Customer Portal. Obtained and inspected communication documentation for a sample O365 customer to ascertain that security, availability, confidentiality, and processing integrity information is available on their Customer Portal. Examined published documentation for O365 service health center to ascertain that security, availability, confidentiality, and processing integrity information is available to all customers. 	No Exceptions Noted
CA-16 – Customers can report issues and potential incidents by creating a service request through the admin portal, which includes the option for telephone support. Service request status and activity can be viewed through the Admin Center.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that customers can report security, availability, confidentiality, and processing integrity incidents by calling the Customer Support Services (CSS) phone number, or by submitting the incident through the Microsoft website. Obtained and inspected O365 customer service websites and policies to ascertain the existence of a website and phone number through which O365 customers are able to report their security, availability, confidentiality, and processing integrity incidents. Observed the Admin Center portal and ascertained that there was the ability to submit a support request ticket for customer incidents or questions. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-17 – Office 365 adheres to Microsoft Security Policy, which is owned by the Information Risk Management Council (IRMC) comprised of business and security leaders across the company and approved by the IRMC chair, who is also the Chief Information Security Officer (CISO) of Microsoft. This policy defines accountability and responsibility for implementing security and evaluating efficacy of security controls. It addresses asset classification (to include data), risk assessment, access control, change control and acceptance, incident response, exceptions, training, and where to go for additional information. The policy is available on the intranet.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that the Microsoft Security Policy, which defines accountability for implementing security and evaluating security controls, is available on the intranet and adhered to by O365 personnel. • Obtained and inspected the Microsoft Security Policy to ascertain that it is available to personnel on the intranet and defines responsibilities for implementing and overseeing security and related security controls. • Obtained and inspected policy documentation to ascertain that the Microsoft Security Policy is approved by the Information Risk Management Council chair, the Chief Information Security Officer of Microsoft. 	No Exceptions Noted
<p>CA-18 – Changes and software releases within the Office 365 environment are documented / tracked and are approved prior to implementation into production.</p>	<ul style="list-style-type: none"> • Inquired of Change Management control owners that procedures have been established and are followed prior to deploying changes to the production environment. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes are documented and tracked within a tracking tool. • Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that deployed changes were approved by appropriate stakeholders prior to release. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-19 – For teams utilizing the Developer / Operations model, monitoring processes or system configurations are in place to identify and remediate unapproved changes to production.	<ul style="list-style-type: none"> Inquired of Change Management and Logical Security control owners that for the teams using the Developer / Operations model, restrictions are in place to monitor or limit access to implement unapproved changes. Observed that monitoring is in place for developers with access to the environment. Obtain and inspected source code and change ticketing systems to ascertain that system configurations and procedures were in place to identify and remediate unapproved changes. 	No Exceptions Noted
CA-20 – Emergency changes to the production environment follow an emergency change approval process.	<ul style="list-style-type: none"> Inquired of Change Management control owners that deployed emergency changes are approved by identified key stakeholders prior to release into production. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that emergency changes were approved by identified key stakeholders. 	No Exceptions Noted
CA-21 – Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.	<ul style="list-style-type: none"> Inquired of Change Management control owners that testing of changes is documented and required for deployment into production. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that changes are tested prior to release according to established procedures. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that testing was reviewed and approved prior to release according to established procedures. 	OSI Testing carried out for one out of twenty-five samples was not properly retained. All Other Services No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-22 – Microsoft takes a deliberate approach to risk management and annually conducts a risk assessment. The purpose is to identify and prioritize the threats facing O365 and prioritize the most preeminent risks based on impact, likelihood, and management’s controls. Additionally, clear ownership is established for each risk and its mitigation strategy. This is reviewed annually by O365 management with ownership assigned out to individual teams and their management.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that a risk assessment and management process has been established for O365 to identify risks related to security, availability, confidentiality, and processing integrity, and is performed and approved on an annual basis. • Obtained and inspected the Risk Management process and policy documents for evidence that a process has been established. • Obtained and inspected the Risk Assessment for Fiscal Year 2021 completed by the O365 team for evidence that the assessment had been completed and risks have been identified. • Obtained and inspected the approvals by O365 management associated with the completion of the Risk Assessment performed. 	No Exceptions Noted
<p>CA-23 – Risk mitigation strategies and controls that are identified through the annual risk assessment are tracked and reviewed by the assigned owner on a periodic basis.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that a process has been established to track and mitigate risks identified as part of Risk Management process. • Obtained and inspected that for a selection of the risks identified a risk mitigation strategy has been established and has been put in place. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-24 – Effectiveness of existing controls are assessed internally, through risk assessments, vulnerability scanning, and other methods, as well as by third parties on an annual basis. Findings are addressed with corrective actions, which are tracked to and completed in a timely manner.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that the effectiveness of existing controls are assessed, both internally and externally, on an annual basis. Further ascertained per inquiry that any findings from these control assessments are addressed with corrective action plans and tracked through to timely resolution. • Obtained and inspected assessment and review reports to ascertain that external control effectiveness reviews are performed and selected a sample of findings from those reviews to test that corrective action plans were developed and tracked for the findings. • Obtained and inspected risk assessment and security scanning reports to ascertain that vulnerability scans and internal risk assessments were performed and selected a sample of findings from those assessments to test that the issues were tracked through to resolution. 	No Exceptions Noted
<p>CA-25 – Based on meetings with CELA (Corporate, External, and Legal Affairs) and other Microsoft groups, the Office 365 Governance, Risk, and Compliance team updates the control framework to meet regulatory, industry, or technology changes.</p>	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that the O365 control framework is updated as needed to accommodate regulatory, industry, or technology changes. • Obtained and inspected meeting invites and meeting notes demonstrating that the Governance, Risk & Compliance group met with Microsoft regulatory groups, including CELA (Corporate, External, and Legal Affairs), to discuss regulatory, industry, and technology changes. • Obtained and inspected meeting invites and meeting notes to ascertain that service teams reviewed the O365 control framework with the point of contacts and updated the framework accordingly. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>CA-26 – Processes and procedures have been established to report security incidents to the Security team. Security incidents are identified and tracked until resolution in an incident tracking system.</p>	<ul style="list-style-type: none"> • Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. • Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review. • Obtained and inspected incident documentation for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken. 	<p>No Exceptions Noted</p>
<p>CA-27 – There is a continual process for host vulnerability scanning, reporting and management review. Individual or centralized services apply patches and remediate vulnerabilities, which is verified and reported to management through a centralized process. Responses are tracked from compliant and non-compliant hosts, to insure timely resolution of incidents of non-compliance.</p>	<ul style="list-style-type: none"> • Inquired of Monitoring and Incident management process owners that processes for security vulnerability scanning have been established and outline requirements for addressing identified issues. • Obtained and inspected security scanning reports that vulnerability scans were being performed and completing successfully over the O365 environment. • Obtained and inspected security scanning reports for a selected date to ascertain that scan results were being reviewed and issues noted were being tracked to resolution. 	<p>No Exceptions Noted</p>

Control Activity	Tests Performed	Test Result
<p>CA-29 – Each Service team has on-call personnel who respond to potential Security, Availability, Confidentiality, and Processing Integrity incidents. If an incident is assigned a high severity, the O365 Security team will track and address the issues to resolution.</p>	<ul style="list-style-type: none"> • Inquired of Operations process owners to ascertain that each workload has on-call personnel established to identify and assist in security, availability, confidentiality, and processing integrity incidents. • Observed and inspected the on-call listing for each workload for evidence that on-call personnel have been established and the on-call personnel covers a 24 hours / 7 days schedule. • Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. • Obtained and inspected incident documentation for a selection of incidents to ascertain that identified high severity security incidents were documented within an incident tracking system and resolved. 	<p>No Exceptions Noted</p>
<p>CA-30 – Processing capacity and availability are monitored by Service teams through the dashboard. Service capacity and availability incidents are alerted and resolved by the on-call personnel as needed.</p>	<ul style="list-style-type: none"> • Inquired of Operations process owners to ascertain that each workload has established a dashboard for monitoring capacity and availability. • Observed and inspected the capacity and availability dashboards for each workload for evidence that capacity and availability metrics are being tracked and displayed to identify service-related issues. • Obtained and inspected an example automated availability alert to ascertain that alerting is in place and incidents are resolved as needed. • Obtained and inspected incident documentation for a selection of incidents to ascertain that capacity and availability incidents were escalated and reviewed by the appropriate team and required action was taken. 	<p>No Exceptions Noted</p>

Control Activity	Tests Performed	Test Result
CA-31 – Office 365 management reviews capacity and availability on a monthly basis. Any issues with or changes to capacity and availability are tracked to resolution.	<ul style="list-style-type: none"> Inquired of Operations and Governance, Risk & Compliance process owners to ascertain that capacity and availability are reviewed on a monthly basis by O365 management. Obtained and inspected that for a selection of Monthly Service Review meetings, O365 management reviews capacity and availability issues on a monthly basis. 	No Exceptions Noted
CA-32 – Access to shared accounts within the Office 365 environment are restricted to authorized personnel.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that shared accounts within the workloads are restricted to authorized personnel. Obtained and inspected logging and monitoring documentation and security configurations to ascertain that shared user accounts are identified and managed by the workloads to restrict access to authorized personnel. 	No Exceptions Noted
CA-33.a – Requests for new access, or modifications to existing access, are submitted and approved prior to provisioning employee, contractor, and service provider access to specific applications or information resources.	<ul style="list-style-type: none"> Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted. Identified population of users whose access had been modified or granted during the reporting period. Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-33.b – Elevated access within the O365 production environment is approved by an authorized user.	<ul style="list-style-type: none"> • Inquired of Logical Access control owners that processes have been established for requesting and approving access prior to access being granted. • Observed and inspected the system configurations for elevated access within the O365 production environment to ascertain that elevated access is restricted to only approved individuals and is limited based on the established time constraints (for Just in Time Systems). • For Just in Time Systems - Observed for a sample of one user per just in time system that the individual was approved prior to access being elevated, and that the access duration was limited to the requested time. • For Standing Access Systems - Obtained and inspected access request documentation for a selection of users to ascertain that a request for access was submitted and authorized prior to implementation. 	No Exceptions Noted
CA-34 – Identity of users is authenticated to Office 365 Services. The use of passwords incorporates policy on periodic change and password complexity.	<ul style="list-style-type: none"> • Inquired of Logical Access control owners that authentication processes and password policies are enforced. • Observed system configuration settings for a selected server for each service to ascertain that authentication policies regarding change intervals and complexity are being enforced. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.a – Access to privileged accounts is configured to be revoked automatically based on access expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation.	<ul style="list-style-type: none"> Inquired of the O365 team that processes have been established for identity access management system configuration to revoke access automatically based on account expiration settings, including inactivity, Manager / Cost Center changes, group settings, and certificate rotation. Obtained and inspected source code of the system configurations within the identity access management tools to corroborate that account expiration settings, including inactivity, Manager / Cost Center changes, and group settings are configured to remove access. Obtained and inspected system logs and tracking tickets for selected individuals that expiration settings were enforced, and access was removed based on the configurations within the identity access management system. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.	<ul style="list-style-type: none"> Inquired of the O365 team that processes have been established for reviewing elevated access that is not automatically expired. Obtained and inspected user access review documentation for selected quarters to ascertain that access was reviewed, and any identified issues were addressed in a timely manner. With regards to the testing exceptions, obtained and inspected the alert logs for user access to the IC3 Azure environments supporting SfB and Microsoft Teams during the examination period to ascertain that no inappropriate access or changes were made during the period, and any alerts generated were tracked and resolved in a timely manner. 	<p><u>IDM</u> User access reviews were not properly documented from Quarter 1 through Quarter 3.</p> <p><u>WAC</u> For the selected Quarter 1 and Quarter 3 reviews, noted that two of 35 users marked for modification / removal were not removed in a timely manner during the Quarter 3 user access review.</p> <p><u>SfB / Microsoft Teams</u> The quarterly user access reviews supporting the Skype for Business and Microsoft Teams services did not include all relevant access groups related to its supporting services' Azure environments.</p> <p><u>All Other Services</u> No Exceptions Noted</p>
CA-36 – Authentication over an encrypted Remote Desktop Connection is used for administrator access to the production environment.	<ul style="list-style-type: none"> Inquired of Logical Access owners to gain an understanding of how authentication is enforced, and processes established with relation to encrypting communication with the production environment. Observed authentication to a selected production server to corroborate that two-factor authentication was required. Obtained and inspected source code configurations and system settings corroborating the encryption settings enforced for accessing the production environment. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-37 – Each Office 365 Service customer’s content is segregated either logically or physically from other Online Services customers’ content.	<ul style="list-style-type: none"> • Inquired of security process owners to gain an understanding of the processes that enforce segregation, either physically or logically, of customer content. • Obtained and inspected a sample of physical server configurations and tested user interfaces to ascertain that customer content is segregated. 	No Exceptions Noted
CA-38 – Production servers go through a quality assurance review prior to installation in the production environment to confirm the server is configured in compliance with baseline security and operational settings according to the server’s intended use.	<ul style="list-style-type: none"> • Inquired of Server Build-out management process owners that processes have been established to have baseline security and operational settings applied to all new servers deployed to the production environment. • Obtained and inspected system logs, source code configurations, and system change documentation for a selection of new servers to ascertain that baseline builds have been established, approved, and deployed prior to a new server being implemented in production. 	No Exceptions Noted
CA-39 – User groups and access control lists have been established to restrict access to Microsoft Datacenters-managed network devices.	<ul style="list-style-type: none"> • Inquired of Global Networking Services (GNS) process owners to ascertain that procedures are in place for restricting access to Microsoft Datacenters managed network devices. Inquired that user groups have been created and enforced via the Active Directory. • Obtained and inspected a sample of network devices and inspected their configuration and tested that TACACS+/Radius are used for authentication, authorization of access and that ACLs have been applied. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-40 – Access to Microsoft Datacenters-managed network devices is restricted through a limited number of entry points that require authentication over an encrypted connection.	<ul style="list-style-type: none"> Inquired with the GNS process owners to ascertain that access to the network devices in the Microsoft Datacenters environment is restricted through a limited number of entry points which require authentication over an encrypted Remote Desktop connection. Inspected the GNS Account Management SOP and tested that procedures are established to restrict user access to Microsoft Datacenters-managed network devices in the scope boundary, through a limited number of entry points that require authentication over an encrypted connection. Selected a sample of Microsoft Datacenters-managed network devices and tested that remote access to network devices involves login to GNS RDG, using domain credentials and Smart card followed by login to internal-facing terminal server using domain credentials and Secure Shell (SSH) has been enforced to access the network device. Obtained the list of terminal servers and tested that access to network devices is restricted through a limited set of terminal servers. Selected a sample of network devices and inspected their configuration and tested that device access is restricted via above terminal servers. 	No Exceptions Noted
CA-41 – A Access to Microsoft Datacenters-managed network devices requires two-factor authentication or other secure mechanisms.	<ul style="list-style-type: none"> Inquired of GNS process owners to ascertain that two-factor authentication is enforced while connecting to a network device. Selected a sample of network devices and observed that login to these network devices required two-factor authentication. Inspected obtained device configuration files for a selection of network devices to ascertain that they were configured to enforce two-factor authentication through TACACS+ or RADIUS servers. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-43 – When users no longer require access or upon termination the user access privileges are revoked in a timely manner.	<ul style="list-style-type: none"> Inquired of security management to gain an understanding of the process for disabling or removing access in a timely manner. Compared a listing of all terminated/ transferred users within the examination period with active user accounts in O365 environments to ascertain if access for terminated/ transferred employees was revoked. Additionally, compared HR Termination reports to O365 security groups to ascertain that removals of terminated users were executed in a timely manner by comparing the users' termination dates against the date of access revocation. 	No Exceptions Noted
CA-44 – Data in motion is encrypted when transmitting data between the customer and the data center and between data centers.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that for workloads that transmit customer content, these transmissions are performed using encryption. Obtained and inspected the encryption settings and certificates that are established over the customer content transmission paths for the applicable workloads. Obtained and inspected the encryption settings and certificates that are established over the datacenter transmission paths for the applicable workloads. 	No Exceptions Noted
CA-45 – Antimalware detects and prevents introduction of known vulnerabilities and quarantines infected systems. Antimalware signatures are updated as available.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that Antimalware has been installed, is running, and is up to date within the O365 environment. Obtained and inspected that for a selection of one server per service team, Antimalware programs have been installed, are running, and are up to date. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-46 – Production releases undergo a security review prior to their release into the production environment per defined criteria, including a code review.	<ul style="list-style-type: none"> Inquired of SDL security process owners to ascertain that changes undergo a security review prior to release. Obtained and inspected change tickets and supporting documentation for a selection of changes to ascertain that a security review was performed prior to release for each build. 	No Exceptions Noted
CA-47 – Security events escalated to the Security team are reviewed by the Security Incident Response Team and action is taken in accordance with the established incident response program procedures.	<ul style="list-style-type: none"> Inquired of Monitoring and Incident management process owners that processes for identifying, reporting, and responding to security incidents have been established. Obtained and inspected incident documentation for a selection of incidents to ascertain that identified security incidents were documented within an incident tracking system and resolved. Inquired of Monitoring and Incident management process owners that processes for addressing security incidents have been established and include processes for escalation and review. Obtained and inspected incident documentation for a selection of incidents to ascertain that security incidents were escalated and reviewed by the appropriate team and required action was taken. 	No Exceptions Noted
CA-48 – Microsoft Datacenters-managed network devices are configured to log and collect security events and are monitored for compliance with established security standards.	<ul style="list-style-type: none"> Inquired of Microsoft Datacenters and Online Services Security & Compliance (OSSC) process owners that network devices are configured to log and collect security events and monitored for compliance with established security standards. Observed that logging of security events is automated through a security log database. Additionally, observed security events from a sample server are logged as they occur in the security log database. Obtained and inspected system configurations for a sample of servers and ascertained that the servers were configured to log and collect security events and those logs are monitored for compliance and any necessary items are resolved. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-49 – Procedures have been established for local redundant storage and/or other redundancy measures supporting the availability of applications and customer content.	<ul style="list-style-type: none"> Inquired of Data Backup and Restoration process owners that processes have been established for data backups and restorations. Obtained and inspected evidence for a selection of backups and replications to ascertain that data backups and replication were occurring according to defined procedures and alternative data instances were available for restoration or failover. 	No Exceptions Noted
CA-50 – Service teams participate in Business Continuity programs, which specify, based on criticality, recovery objectives, testing requirements (up to full data center failover), and remediation timelines.	<ul style="list-style-type: none"> Inquired of Business Continuity process owners to ascertain that failover tests occur on a regular basis. Obtained and inspected business continuity documentation and failover logs for a selection of failover tests to ascertain that the tests were completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution. 	No Exceptions Noted
CA-51 – Customer content and services are replicated to a geographically separate location.	<ul style="list-style-type: none"> Inquired of Data Backup and Restoration process owners to gain an understanding of the process for locating customer content on replicated instances in geographically separate locations. Obtained and inspected system configurations and depending on the setup of the service, a selection of data sources, to ascertain that replicated instances reside in geographically separate locations. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-53 – Office 365 monitors its dependencies on Microsoft Azure through obtaining and evaluating attestation reports when available.	<ul style="list-style-type: none"> • Inquired of Governance, Risk & Compliance process owners to ascertain that O365 monitors its dependencies on Microsoft Azure, and their compliance with SLAs / contract obligations. • Obtained and inspected meeting minutes and supporting documentation to ascertain that Audit Reports for each of the dependent Microsoft Azure were obtained and inspected for issues. Any issues identified were followed-up on with the required party. • Obtained and inspected meeting minutes and supporting documentation to ascertain that O365 monitors the dependencies on Microsoft Azure through the scheduled Office Hours meetings. 	No Exceptions Noted
CA-54 – Data at rest is encrypted per policy.	<ul style="list-style-type: none"> • Inquired of Operations and Security process owners to ascertain that for workloads that retain customer content, data at rest has been encrypted. • Obtained and inspected the encryption settings are established over the customer content at rest for the applicable workloads. • Observed for a selected server for each workload that the data stored on the server has been encrypted per policy. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-55 – Customer content is retained after termination of Office 365 subscriptions per agreed upon commitments with the customer in the contract and Service Licensing Agreements.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that for workloads that retain customer content, data is removed per customer agreements when the customer's account is deactivated. Obtained and inspected the system configurations for the applicable workloads that synchronizes customer account status (e.g., Active, Suspended) between Microsoft Azure and the workload. Obtained and inspected system configurations and customer account status logs to ascertain that each applicable workload is configured to systematically remove customer's data based on their account status and is in line with the agreed upon customer's contract and Service Licensing Agreements. 	No Exceptions Noted
CA-56 – Customer tenant administrators are automatically notified when a Customer Lockbox elevation request is initiated to access their content. The tenant administrator must authorize the access elevation request prior to access being granted to the content.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that Customer tenant administrators are notified when a Customer Lockbox elevation request is initiated to access their content. Observed for a selected Customer Lockbox subscriber, that a Lockbox request was submitted and approved by tenant management. 	No Exceptions Noted
CA-57 – Customer Lockbox elevation requests require management approval prior to submission to the tenant administrator.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that customer Lockbox elevation requests require management approval prior to submission to the tenant administrator. Obtained and inspected an access elevation log request and noted approvers were assigned to the request. Obtained and inspected access elevation logs to ascertain that an approval took place before access was granted. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-58 – Customer Lockbox elevation requests to customer content require an associated service request.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that Customer Lockbox elevation requests to customer content require an associated service request. Observed that when a service request number was excluded, the elevation request failed to be processed. 	No Exceptions Noted
CA-59 – Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain Customer Lockbox elevation requests are displayed in the tenant Office 365 Admin Center. Observed the population of Lockbox requests within the Office 365 Dashboard – Admin Center. 	No Exceptions Noted
CA-60 – The workload where the content is accessed logs the access made by the Microsoft Operator, and the entry can be found in the Audit log search.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that all server that host customer content push audit logs to a repository on a real-time basis. Observed for a sample elevation log that cmdlet activity was logged accordingly. Observed for a sample elevation that it can be identified through the Office 365 Dashboard search functionality. 	No Exceptions Noted
CA-61 – Microsoft management reviews both Customer Lockbox and capacity server elevation logs and investigates any anomalies. All elevations statistics are aggregated, reviewed, and reported to management monthly.	<ul style="list-style-type: none"> Inquired of Operations and Security process owners to ascertain that management reviews both Customer Lockbox and capacity server elevation. Obtained and inspected a sample of MSR monthly presentations which included elevation statistics and resolutions. Inspected that an approval was required in advance of an elevation request. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-62 – Customer mailboxes are encrypted per customer’s defined encryption policies using keys generated and maintained by the customer.	<ul style="list-style-type: none"> Inquired with the Customer Key owners to ascertain that each customer is responsible for initiating their service encryption configuration during the Customer Key onboarding process. Observed a test occurrence of a customer’s Customer Key subscription termination process within the production environment to ascertain the customer data was no longer accessible after the tenant’s termination of the Customer Key subscription. 	No Exceptions Noted
CA-63 – When a customer requests a data deletion using the Exchange Customer Key service, the data is no longer accessible by Microsoft or the end user.	<ul style="list-style-type: none"> Inquired with Customer Key owners to ascertain that each customer ‘Customer Key’ subscription has a unique service encryption identifier and a unique Azure Key Vault to house their root encryption keys. Obtained and inspected a sample customer ‘Customer Key’ subscription and ascertained that each of the customer’s service encryptions was associated with unique Azure Key Vaults for the respective encryption root keys. Observed a test occurrence of a failed customer attempt to access an Azure Key Vault that was not associated with their ‘Customer Key’ service encryption. 	No Exceptions Noted
CA-64 – Only keys noted in the tenant’s Data Encryption Policy can be used to access the data maintained in that tenant’s service encryption.	<ul style="list-style-type: none"> Inquired with SharePoint and Exchange service engineers to verify each service account use is logged and monitored. Observed a user successfully access the Data Encryption Policy associated with the service encryption they were provisioned to and observed that same user’s failed attempt to access another service encryption of which the user was not provisioned to. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
CA-65 – Customer content resides in a specific geographic location.	<ul style="list-style-type: none"> Inquired with SharePoint and Exchange service engineers to verify that the SharePoint and Exchange services are configured to restrict customer content to defined geographic regions. Obtained and inspected a sample of geographic regions for both the SharePoint and Exchange services and obtained evidence to ascertain that datacenter and service configurations were setup to restrict customer content to defined regions within each service. 	No Exceptions Noted
CA-66 – Production data is classified and protected based upon the Office 365 data classification process.	<ul style="list-style-type: none"> Inquired of Governance, Risk & Compliance process owners to ascertain that O365 has an established data classification process. Obtained and inspected the data classification standard to ascertain that there is a defined O365 data classification process and associated documentation that service teams can use to track and understand the data that they manage, and the associated security, availability, confidentiality, and processing integrity requirements associated with that data. 	No Exceptions Noted
ELC-01 – Microsoft’s values are accessible to employees via the Values SharePoint site and are updated as necessary by management.	<ul style="list-style-type: none"> Inquired of Microsoft management regarding Microsoft’s values and the process for updating and making them accessible to employees. Observed the Values SharePoint site and ascertained that Microsoft’s values are defined, updated as needed, and published to employees. 	No Exceptions Noted
ELC-02 – Microsoft maintains several mechanisms (email, phone, fax, website) that permit employees and non-employees to communicate confidential and / or anonymous reports concerning Business Conduct.	<ul style="list-style-type: none"> Inquired of Microsoft Office of Legal Compliance (OLC) team regarding the mechanisms (email, phone, fax, website) that permit reporting of issues related to Business Conduct. Accessed each communication mechanism to ascertain that the mechanisms were available and functioning. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>ELC-03 – The Audit Committee (AC) reviews its Charter and Responsibilities as listed in its calendar on an annual basis. The AC Responsibilities include meeting with the external and internal auditors on a quarterly basis; providing oversight on the development and performance of controls; and completing an annual self-evaluation.</p>	<ul style="list-style-type: none"> • Inquired of the members of the Audit Committee (AC) to gain an understanding of the Charter and Responsibilities of the Audit Committee and its annual review process. • Obtained and inspected the agenda or meeting minutes to ascertain the annual review of Audit Committee’s Charter and Responsibilities Calendar. • Inspected the investor relations website to ascertain that the Audit Committee’s Charter and Responsibilities Calendar was published on the website. • Obtained evidence (e.g., meeting invite, meeting minutes) to ascertain quarterly meetings between AC and internal / external auditors. 	No Exceptions Noted
<p>ELC-04 – Internal Audit Charter directs Internal Audit to provide independent and objective audit, investigative, and advisory services designed to provide assurance that the company is appropriately addressing its risks. The scope and frequency of assurance activities is based on an annual risk assessment.</p>	<ul style="list-style-type: none"> • Inquired of Microsoft management to gain an understanding of the Internal Audit Charter and the scope and frequency of assurance activities performed by Internal Audit. • Obtained and inspected the Internal Audit Charter and ascertained that the Charter directs the services of the Internal Audit. 	No Exceptions Noted
<p>ELC-06 – The Compensation Committee is responsible for reviewing and discussing plans for executive officer development and corporate succession plans for the CEO and other executive officers.</p>	<ul style="list-style-type: none"> • Inquired of the members of the Compensation Committee to gain an understanding of the process for planning of executive officer development and corporate succession plans for the CEO and other executive officers. • Obtained and inspected the agenda or meeting minutes to ascertain the annual discussion of the succession plans. • Inspected the Compensation Committee Charter on the investor relations website to ascertain that the Compensation Committee’s responsibility included reviewing the succession plan for CEO and other executive officers, on an annual basis. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>ELC-07 – The Enterprise Risk Management Office (ERMO) has established an entity wide risk assessment process to identify and manage risks across Microsoft. Risk assessment results are reviewed bi-annually and risks that exceed acceptable thresholds are reported to the Board of Directors on behalf of senior management.</p>	<ul style="list-style-type: none"> • Inquired of the Enterprise Risk Management (ERM) team on the ERM risk assessment process and how risks are identified and managed. • Obtained and inspected the agenda or meeting minutes to ascertain that the ERM risk assessment results are reviewed bi-annually and presented to the Board of Directors for review and consideration of the changes. 	No Exceptions Noted
<p>ELC-08 – Microsoft requires employees and contractors to sign agreements that include non-disclosure provisions and asset protection responsibilities, upon hire. In addition, employees are provided Microsoft's Employee Handbook, which describes the responsibilities and expected behavior with regard to information and information system usage, including the consequences of violating relevant laws, regulations, provisions, and policies regarding information security. Employees are required to acknowledge agreements to return Microsoft assets upon termination.</p>	<ul style="list-style-type: none"> • Inquired of the Human Resources (HR) team that Non-Disclosure Agreements (NDAs), that include asset protection and return responsibilities, were signed as a part of the onboarding process. • Inspected a sample NDA to ascertain that the agreement included requirements for asset protection, and asset return upon termination of employment. • Obtained and inspected the Reporting Concerns About Misconduct policy, to ascertain if policies around notification of incidents were documented. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>ELC-09 – Microsoft’s Enterprise Business Continuity program is intended to ensure that Microsoft is ready to mitigate risks and vulnerabilities and respond to a major disruptive event in a manner that enables the business to continue to operate in a safe, predictable, and reliable way. The BCM charter provides a strategic direction and leadership to all Microsoft Engineering organizations. BCM is governed through the Program Management Office to ensure that the program adheres to a coherent long-term vision and mission, and is consistent with enterprise program standards, methods, policies, and metrics.</p>	<ul style="list-style-type: none"> • Inquired of Business Continuity process owners to ascertain that Office 365 teams participate in the Enterprise Business Continuity program and abide by the BCM charter • Obtained and inspected that for a selection of failover tests, that the test was completed as designed, and that any issues identified were assigned to an appropriate owner and being tracked to resolution. 	No Exceptions Noted
<p>ELC-10 – Teams evaluate changes according to criteria defined by GRC. Changes that meet the criteria go through a review that includes a risk assessment.</p>	<ul style="list-style-type: none"> • Inquired of workstream control owners regarding how they evaluate changes to see if they require a risk assessment. • Obtained and inspected risk assessments completed as part of Office Hours to ascertain that for each workstream a risk assessment would be performed for changes based on GRC defined criteria. 	No Exceptions Noted
<p>ELC-11 – Audit activities are planned and agreed upon in advance by stakeholders and any access required to perform the audits requires approval. Audit findings are addressed relative to their criticality.</p>	<ul style="list-style-type: none"> • Inquired of GRC process owners regarding their process for planning and executing audit activities. • Obtained and inspected evidence from the most recent ISO audit of the O365 Germany system to ascertain that an audit plan was defined, corroborate that any access required to perform the audit was approved, and that audit findings were addressed. 	No Exceptions Noted

Control Activity	Tests Performed	Test Result
<p>ELC-12 – Management expects outsourced providers to meet certain levels of skills and experience, depending on the role and holds them accountable to achieving specific deliverables, as outlined in the Statement of Work template. Including understanding the consequences of violating relevant laws, regulations, provisions, and policies regarding information security.</p>	<ul style="list-style-type: none"> • Inquired of Microsoft management regarding the process for: <ul style="list-style-type: none"> - Citing expectations from outsourced providers to achieve specific deliverables - Training outsourced providers on Microsoft’s supplier code of conduct • Obtained and inspected Microsoft’s Statement of Work template to ascertain that it cited outsourced providers’ role and accountability in achieving specific deliverables. • Inspected the supplier procurement website to ascertain that Microsoft’s supplier code of conduct is available and accessible to all outsourced providers. • Obtained and inspected the Standards of Business Conduct training transcript to confirm that for all internal employees, obligations are communicated as part of the Standards of Business Conduct training. • Observed during the supplier access provisioning process that completion of the supplier code of conduct training is required. 	No Exceptions Noted
<p>ELC-15 – Security risks related to external parties (such as customers, contractors and vendors) are identified and addressed within the Office 365 environment based on Microsoft’s corporate procurement process. Designated responsibilities are defined to coordinate with relevant corporate groups (e.g., Corporate, External, and Legal Affairs, Procurement) in reviewing risks associated with external parties and establishing relevant agreements.</p>	<ul style="list-style-type: none"> • Inquired of process owners regarding their risk assessment process and how risks are identified and addressed related to external parties (such as customers, contractors and vendors). • Obtained and inspected the latest risk assessment performed by Microsoft Azure management to ascertain that it was complete. • Obtained and inspected the Statement of Work (SOW) template citing external parties’ access was restricted authoritatively based on the risk assessment performed. 	No Exceptions Noted

Section V:

Supplemental Information Provided by Microsoft

The information included in this section is presented by Microsoft Corporation (“Microsoft”) to provide additional information to user entities and is not part of Microsoft’s description of the system. The information included here in this section has not been subjected to the procedures applied in the examination of the description of the system, and accordingly, Deloitte & Touche LLP expresses no opinion on it.

Business Continuity Planning

The Microsoft Office 365 (“O365”) service incorporates resilient and redundant features in each service and utilizes Microsoft’s enterprise-level datacenters. These datacenters use the same world-class operational practices as Microsoft’s corporate line of business applications. The O365 team’s long experience in operating highly available services, combined with the company’s close ties to the product groups and support services, provides a comprehensive solution for the company’s online services with the ability to meet the high standards of its customers.

The company’s online services designs include provisions to quickly recover from unexpected events such as hardware or application failure, data corruption, or other incidents that may affect a subset of the user population. The company’s service continuity solutions and framework are based on industry best practice and are updated on a regular basis to support Microsoft’s ability to recover from a major outage in a timely manner.

Domain Name Services

O365 Domain Name Service (DNS) provides authoritative name resolution for a subset of public-facing domains associated with O365. These domains can be purchased by customers to rename their domain URLs.

Datacenter Services

The Microsoft Datacenters Management team has overall responsibility for the oversight of datacenter operations, including physical security, site services (server deployments and break/fix work), infrastructure build-out, critical environment operations and maintenance, and facilities management. Site Security Officers are responsible for monitoring the physical security of the facility 24x7.

The Microsoft Datacenters Management team conducts periodic operational reviews with the key third-party vendors that support the Microsoft Datacenters. The purpose of the operational reviews is to discuss the current state of agreed-upon deliverables. Third-party vendors have specific statements of work with service level agreements that are monitored for compliance and adherence. Statements of work are reviewed on a periodic basis and updates are made accordingly, as business needs require.

ISO/IEC Standards 27001:2013, 27017:2015, and 27018:2014

O365 is compliant with ISO standard 27001:2013 and meets the requirements of ISO 27017:2015 and 27018:2014, published jointly by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC).

ISO27000 series of standards were developed in the context of the following core principles:

“The preservation of confidentiality (ensuring that information is accessible only to those authorized to have access), integrity (safeguarding the accuracy and completeness of information and processing methods) and availability (ensuring that authorized users have access to information and associated assets when required).”

O365 has undergone the ISO 27001 certification process and has been certified by the British Standards Institute (BSI). To view the ISO/IEC 27001:2013 certificates, see the Certificate/Client Directory Search Results page located on the BSI Global website.

NIST 800-53 and FISMA

O365 implements security processes and technology that adhere to the NIST 800-53 standards required by US federal agencies and have acquired FedRAMP Authority to Operate (ATO) from multiple federal agencies.

Management's Response to Exceptions Identified

The table below contains Management's responses to the exceptions identified in **Section IV**.

Control Activity & Exception	Management's Response
<p>CA-35.b – Elevated access within the O365 environment that is not subject to automatic expiration settings is manually reviewed on a periodic basis.</p> <p><u>IDM</u> User access reviews were not properly documented from Quarter 1 through Quarter 3.</p> <p><u>WAC</u> For the selected Quarter 1 and Quarter 3 reviews, noted that two of 35 users marked for modification / removal were not removed in a timely manner during the Quarter 3 user access review.</p> <p><u>SfB / Microsoft Teams</u> The quarterly user access reviews supporting the Skype for Business and Microsoft Teams services did not include all relevant access groups related to its supporting services' Azure environments.</p>	<p><u>IDM, WAC, SfB / Microsoft Teams</u> Logs of account usage have been reviewed. Confirmed that there has been no usage of the expired accounts since their last authorized usage date. Applicable teams have been reminded of this control requirement.</p>
<p>CA-21 (2.04) - Testing is carried out on all changes according to established procedures. Users and stakeholders review and approve results of testing prior to implementation.</p> <p><u>OSI</u> Testing carried out for one out of twenty-five samples was not properly retained.</p>	<p>Confirmed builds subsequent to the undocumented example followed required test procedures and found no residual faults. We have increased the retention time for this system.</p>

ASUS EXHIBIT G

Cross Country
Computer Corp
Certification and
SOC Reports

CERTIFICATE OF REGISTRATION

Information Security Management System

ISO/IEC 27001: 2013

This is to certify that the Information Security Management System of:

Cross Country Computer Corp
250 Carleton Avenue
East Islip, New York 11730

Conforms with the requirements of ISO/IEC 27001: 2013 for the scope listed below:

In accordance with the requirements of ISO standard ISO/IEC 27001:2013, Cross Country's Information Security Management System (ISMS) is required to appropriately preserve the confidentiality, integrity, and availability of information assets owned or managed by Cross Country. The ISMS is managed from Cross Country's New York headquarters. The ISMS framework serves as Cross Country's mechanism to identify, select, maintain, and improve information security controls for the following products and services:

- APEARS® death matching
- Database development and hosting
- Data hygiene and merge purge
- E-mail services
- Multi-channel matchback
- List rental fulfillment
- Strategy and analytics
- Unclaimed property compliance

Certificate Number: SEC1596 v2.0

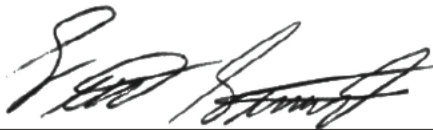
Statement of Applicability: 16.2 (08/26/2016)

Recertification Date: 01/05/2020

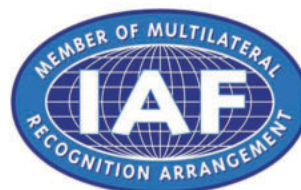
Expiry Date: 01/06/2023

Original Registration Date: 01/06/2017

Issued by:



EVP, Compliance Services



This certificate was issued electronically and is bound by the terms and conditions set forth in the agreement. Further clarification regarding the scope of this certificate and applicability to the ISO/IEC 27001: 2013 standard may be obtained at www.a-lign.com.

A-LIGN Headquarters: 400 N. Ashley Dr. Suite 1325 Tampa, Florida 33602 Tel: 888-702-5446



A-ALIGN



Cross Country Computer Corp.
Type 1 SOC 2 with
HIPAA/HITECH
2022



**REPORT ON CROSS COUNTRY COMPUTER CORP.'S DESCRIPTION OF ITS
SYSTEM AND ON THE SUITABILITY OF THE DESIGN OF ITS CONTROLS
RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY
WITH HIPAA/HITECH REQUIREMENTS**

**Pursuant to Reporting on System and Organization Controls 2 (SOC 2)
Type 1 examination performed under AT-C 105 and AT-C 205**

January 15, 2022

Table of Contents

SECTION 1 ASSERTION OF CROSS COUNTRY COMPUTER CORP. MANAGEMENT.....	1
SECTION 2 INDEPENDENT SERVICE AUDITOR'S REPORT	4
SECTION 3 CROSS COUNTRY COMPUTER CORP.'S DESCRIPTION OF ITS DATA MANAGEMENT SOLUTIONS SERVICES SYSTEM AS OF JANUARY 15, 2022	8
OVERVIEW OF OPERATIONS.....	9
Company Background	9
Description of Services Provided	9
Principal Service Commitments and System Requirements.....	10
Components of the System.....	11
Boundaries of the System.....	21
RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING	21
Control Environment.....	21
Risk Assessment Process	23
Information and Communications Systems.....	24
Monitoring Controls	25
HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS.....	26
Policies and Procedures	26
Security Awareness Training	26
Periodic Testing and Evaluation	26
Remediation and Continuous Improvement.....	27
Incident Response.....	27
Changes to the System Since the Last Review.....	27
Incidents Since the Last Review	27
Trust Services Criteria and HIPAA/HITECH Requirements Not applicable to the System...	27
Subservice Organizations.....	28
COMPLEMENTARY USER ENTITY CONTROLS.....	34
TRUST SERVICES CATEGORIES.....	35
HEALTH INFORMATION SECURITY PROGRAM	36
CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION	38
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	38
ADDITIONAL CRITERIA FOR THE AVAILABILITY CATEGORY	60
ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY	61
ADMINISTRATIVE SAFEGUARDS	62
PHYSICAL SAFEGUARDS	69
TECHNICAL SAFEGUARDS.....	71
ORGANIZATIONAL REQUIREMENTS	73
BREACH NOTIFICATION	76
SECTION 4 INFORMATION PROVIDED BY THE SERVICE AUDITOR	81
GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR	82

SECTION 1

ASSERTION OF CROSS COUNTRY COMPUTER CORP. MANAGEMENT

ASSERTION OF CROSS COUNTRY COMPUTER CORP. MANAGEMENT

February 16, 2022

We have prepared the accompanying description of Cross Country Computer Corp.'s ('CCC' or 'the Company') Data Management Solutions Services System titled "Cross Country Computer Corp.'s Description of Its Data Management Solutions Services System as of January 15, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the Data Management Solutions Services System that may be useful when assessing the risks arising from interactions with Cross Country Computer Corp.'s system, particularly information about system controls that Cross Country Computer Corp. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

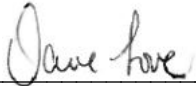
Cross Country Computer Corp. uses 365 Data Centers to provide colocation services and Flexible Business System ('FBS') to provide managed IT services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cross Country Computer Corp., to achieve Cross Country Computer Corp.'s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Cross Country Computer Corp.'s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Cross Country Computer Corp.'s controls. The description does not disclose the actual controls at the subservice organizations.

The description indicates that complementary user entity controls that are suitably designed are necessary, along with controls at Cross Country Computer Corp., to achieve Cross Country Computer Corp.'s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Cross Country Computer Corp.'s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Cross Country Computer Corp.'s controls.

We confirm, to the best of our knowledge and belief, that

- a. the description presents Cross Country Computer Corp.'s Data Management Solutions Services System that was designed and implemented as of January 15, 2022, in accordance with the description criteria.

- b. the controls stated in the description were suitably designed as of January 15, 2022, to provide reasonable assurance that Cross Country Computer Corp.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of Cross Country Computer Corp.'s controls as of that date.



Dave Love
EVP & CSO
Cross Country Computer Corp.

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Cross Country Computer Corp.

Scope

We have examined Cross Country Computer Corp. accompanying description of its Data Management Solutions Services System titled "Cross Country Computer Corp.'s Description of Its Data Management Solutions Services System as of January 15, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), (description criteria) and the suitability of the design of controls stated in the description as of January 15, 2022, to provide reasonable assurance that Cross Country Computer Corp.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). We have also examined the suitability of the design of controls to meet essential elements of the Health Insurance Portability and Accountability Act Security Rule of 2003 ("HIPAA") and the Health Information Technology for Economic and Clinical Health Act ("HITECH"), enacted as part of the American Recovery and Reinvestment Act of 2009.

Cross Country Computer Corp. uses 365 Data Centers to provide colocation services and Flexible Business System to provide managed IT services (collectively, the 'subservice organizations'). The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Cross Country Computer Corp., to achieve Cross Country Computer Corp.'s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Cross Country Computer Corp.'s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the types of complementary subservice organization controls assumed in the design of Cross Country Computer Corp.'s controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Cross Country Computer Corp., to achieve Cross Country Computer Corp.'s service commitments and system requirements based on the applicable trust services criteria and HIPAA/HITECH requirements. The description presents Cross Country Computer Corp.'s controls, the applicable trust services criteria and HIPAA/HITECH requirements, and the complementary user entity controls assumed in the design of Cross Country Computer Corp.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Cross Country Computer Corp. is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Cross Country Computer Corp.'s service commitments and system requirements were achieved. Cross Country Computer Corp. has provided the accompanying assertion titled "Assertion of Cross Country Computer Corp. Management" (assertion) about the description and the suitability of the design of controls stated therein. Cross Country Computer Corp. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and HIPAA/HITECH requirements and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria and HIPAA/HITECH requirements. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based the applicable trust services criteria and HIPAA/HITECH requirements
- Evaluating the overall presentation of the description

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

- a. the description presents Cross Country Computer Corp.'s Data Management Solutions Services System that was designed and implemented as of January 15, 2022, in accordance with the description criteria.

- b. the controls stated in the description were suitably designed as of January 15, 2022, to provide reasonable assurance that Cross Country Computer Corp.'s service commitments and system requirements would be achieved based on the applicable trust services criteria and HIPAA/HITECH requirements, if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Cross Country Computer Corp.'s controls as of that date.

Restricted Use

This report is intended solely for the information and use of Cross Country Computer Corp., user entities of Cross Country Computer Corp.'s Data Management Solutions Services System as of January 15, 2022, business partners of Cross Country Computer Corp. subject to risks arising from interactions with the Data Management Solutions Services System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties
- Internal control and its limitations
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The applicable trust services criteria and HIPAA/HITECH requirements
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE
Tampa, Florida
February 16, 2022

SECTION 3

CROSS COUNTRY COMPUTER CORP.'S DESCRIPTION OF ITS DATA MANAGEMENT SOLUTIONS SERVICES SYSTEM AS OF JANUARY 15, 2022

OVERVIEW OF OPERATIONS

Company Background

Cross Country Computer (CCC) specializes in bringing strategic marketing and data management within the reach of all companies seeking to evolve methods and turn the return on investment (ROI) equation back in favor. Their industry experts and robust data management solutions make it easier for customers to acquire, retain and develop valuable customers.

Since inception in 1975, CCC has matured into a data service provider, specializing in meeting the needs of both business and consumer marketers as well as insurance companies that must comply with death matching legislation. CCC provides strategic advice and accurate solutions needed to meet the challenges of the day. CCC have established many best practices throughout the years and continue to evolve to meet the ever-changing needs of the industries.

Description of Services Provided

CCC is touted as the primary data services provider for almost two hundred clients across many different verticals, many who have grown with CCC for 25+ years:

- Business-to-Consumer (B2C) - Retail / Catalog
- Business-to-Business (B2B) - List Managers
- Advertising Agencies - Financial Services
- Human Resources - Publishers
- Federal Agencies - Insurance

CCC Products & Services

CCC's products and services were designed to address the challenges organizations face and the need they have to employ more sophisticated strategies to remain competitive.

APEARS®

Data management and unclaimed property expertise provides insurers with a proven death matching process leveraging the Social Security Administration's National Technical Information Service (NTIS) Limited Access Death Master File (LADMF) and other sources of death data in a manner that exceeds the fuzzy matching requirements for state mandated compliance.

DM Optimization Suite

Strategic Marketing from Start to Finish. Today's economic challenges have the industry looking for value-based solutions that can help turn the marketing ROI back in its favor. CCC's Database Marketing Optimization Suite provides the insight needed to identify the best targets for customers while streamlining processing and bundling costs for higher margin.

LR Optimization Suite

List Rental Fulfillment Made Easy. List owners and managers challenged by increasing competition, lower margins and more complex demands need to find ways to improve eroding ROI. CCC's all-inclusive turnkey list management solution can help via the provision of quick counts and speedy shipment of orders with integrated split/nth/key capabilities.

CrossSelect™

CrossSelect marketing database brings together disparate data repositories, applies hygiene and aggregation to form new fields and provides customers with 24/7 on-line access for dashboard reporting, ad hoc querying and fast multichannel campaign execution.

CrossMatch™: Understanding Multi-Channel Performance

The rise of new marketing and purchase channels has made it difficult to understand the true drivers of revenue. As a result, campaigns are not linked to purchases and performance is often understated leading to suboptimal decision making. CrossMatch™ is an automated on-line reporting tool which enables marketers to understand what truly drives sales.

cMail™

As marketers turn their focus to cultivation of their own customer base, the role of e-mail as the most cost-effective means of 1:1 marketing today has come into focus. CCC understands the revenue potential associated with this media channel and has tailored a suite of services called cMail™ that works together to ensure DELIVERABILITY and TARGET OPTIMIZATION.

Data Hygiene

Reduce postage costs and improve deliverability with Coding Accuracy Support System (CASS) Certification, Delivery Point Validation (DPV), National Change Of Address (NCOA), Locatable Address Change Service (LACS), Deceased, Prison and related address standardization and suppression services. Identify, correct and classify job titles to improve targeting, delivery, response and ROI with their Title Beautification program.

Merge Purge

CCC understands the need for speed. They embrace automation within their systems that improve quality and reduce in-the-mail cycle time leading to higher response. By eliminating more duplicates, employing smart-key strategies, saving postage costs and reducing in-the-mail cycle time, they help their customers achieve higher returns through optimized targeting at a lower cost. The end result is a higher return on investment and faster database growth.

Strategy & Analytics

Turning Insights into Actions. Gone are the days of replicating last year's marketing plan and expecting the same results. Today's marketer needs to be more strategic, do more with less while achieving the projected profit targets. Now more than ever, marketers turn to data and analytics to provide them with the insights and answers for how best to guide their total marketing budget for maximum ROI. CCC's industry leading strategists are experts at analyzing data and turning findings into actionable solutions for today's business challenges.

Principal Service Commitments and System Requirements

CCC designs its processes and procedures related to its direct marketing and data management solutions to meet their customer commitments, the laws and regulations that govern the provision of these services, and with adherence to the security standards they have instituted.

CCC is dedicated to managing risk through the implementation of, and compliance with, a comprehensive Information Management Security System (ISMS) that meets International Organization for Standardization (ISO)/International Electrotechnical Commission (IEC) 27001:2013 standards and satisfies CCC's HIPAA obligations. Because their clients and partners entrust CCC with a wide range of confidential Personally Identifiable Information (PII), Protected Health Information (PHI) and related sensitive data, it is critical to have proper security controls in place governing all aspects of their business. A single data breach could have devastated impact to CCC's business in areas ranging from client loss to damaged reputation & brand value, legal costs and financial loss which may or may not be adequately covered by insurance. Adherence to this Security Policy and the associated risk management and security procedures are considered to be of paramount importance within their organization.

Applicable are all aspects of CCC's business including staff, designated vendors, facilities, systems, software, and business practices. Material internal and external issues that affect CCC's ability to ensure the integrity of their ISMS include but are not limited to:

- Staff familiarity with CCC's policies & procedures, and consistency in handling deviations
- Regulation of access control privileges to all systems containing confidential information
- Secure transmission, processing, storage, backup and recovery of confidential information
- Proper configuration of firewalls and application of security patches and spam filtering
- Vendor ability to provide and adhere to adequate security representations regarding confidential information
- Applies to outsourced provision of data, e-mail deployment and IT support services
- Leadership overseeing annual Risk Assessments, pursuing improvement & documenting results
- Availability & maintenance of proper insurance coverages as a mechanism to transfer risk

Components of the System

Infrastructure

Primary infrastructure used to provide CCC's Data Management Solutions Services System includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
CCC-ESXi1 Server	Hewlett Packard DL360 Gen9	Virtualized server with a VMware ESXi 5.5 operating system (OS)
CCC-ESXi2 Server	Hewlett Packard DL360 Gen9	Virtualized server with a VMware ESXi 5.5 OS
CCC-ESXi3 Server	Hewlett Packard DL360 Gen9	Virtualized server with a VMware ESXi 5.5 OS
CCC-MSA01 Storage Controller	Hewlett Packard MSA 2040 Fiber Storage Controller	Controls 3 shelves of storage
Sophos SG 210 UTM redundant Firewalls (at Data Center)	Sophos SG 210 unified threat management (UTM)	Filters traffic into and out of the private network supporting the corporate services intrusion prevention system (IPS), Adenosine Triphosphate Phosphocreatine (ATP), Web Filtering
CCC-SWCI1 and CCC-SWEI2 (Switches)	Dell PowerConnect 6224 and a Hewlett Packard 1810	Connects devices on the corporate network by sending message to the specific device(s) that need to receive it

Primary Infrastructure		
Hardware	Type	Purpose
Hewlett-Packard (HP) Aruba 2530 8G Switch - CN65FP81MB	HP Aruba 2530 8G Switch	To facilitate redundant firewalls at Data Center
CCC-DC03 Server	Hewlett Packard ML310e Gen8	At 250 Carleton Ave Office. Primary Domain and Printer Controller
Sophos SG 135 Redundant Firewalls (at Office)	Sophos SG 135	Filters traffic into and out of the private network supporting the corporate services
HP Aruba 2530 8G Switch - CN65FP81MB	HP Aruba 2530 8G Switch	To facilitate redundant firewalls at Office

Software

Primary software used to provide CCC's Data Management Solutions Services System includes the following:

Primary Software		
Software	Operating System	Purpose
Satori (Quadient): Architect, Presort	Windows Server 2012 R2	File Formatting, selecting/omitting, address Hygiene, Postal Presort, Merge Purge
GT Software: NetCOBOL, PowerBsort	Windows Server 2012 R2	Common Business Oriented Language (COBOL) language for developers, Sort tool
DMExpress-Syncsort	Windows Server 2012 R2	Sorting tool, also filters, formats, Sums, etc.
Microsoft Office Standard 2016 (some 2010 as well)	Windows Server 2012 R2, Windows Server 2008	Word, Excel, PowerPoint, etc.
VM Sphere	Windows Server 2012 R2	On 3 physical servers supporting 27 virtual servers
Intuit QuickBooks Pro 2016	Windows Server 2012 R2	Accounting software
WindowBooks TagMaster	Windows Server 2012 R2	Bag and tray Tag producer for Postal Presort output
ManageEngine ADAuditplus	Windows Server 2012 R2	Monitoring application used to provide monitoring, alert and notification services for the hosted client environments
BetrData	Ubuntu - Linux	Data Conversion tool. Actively polls secure file transfer protocol (SFTP) sites, pulls down files, analyzes, converts, and reports on them

People

CCC has a staff of approximately 55 employees. The Executive Team provides senior level guidance to each department as well as strategic planning and budgeting. Responsible for profit and loss (P&L), Security Compliance, IT support.

Client Services - responsible for the day to day direct client management. Includes project management, client request to internal instruction translation, data trafficking, quality control, invoicing.

Production Programming - execution of data management jobs based upon client service specifications. Quality control.

Human Resources - responsible for new employee intake and background check process. Benefits administration, payroll and on-going employee support. Coordination with and management of their professional employer organization (PEO) relationship.

Finance - account payable (A/P), accounts receivable (A/R), purchasing and budgetary reporting.

Applications Development - responsible for writing programs to meet company/client data management needs. Quality control. Responsible for Level 1 helpdesk IT support.

CCC also augments their in-house IT support staff through a contractual partnership with Flexible Business Systems (FBS), a Hauppauge New York based Information Technology services firm dedicated to implementing and maintaining the technology of hundreds of businesses. While CCC is able to manage many support requirements internally, FBS is available as an additional help desk resource and for deployment of larger scale solutions. Their FBS Account Team also has authorization to access CCC's co-lo data center in accordance with the co-lo data center's access control policies when physical server support is required.

Data

When transferring Confidential Information to CCC that includes PII (examples which include customer names & addresses, social security numbers, demographic/firmographic data, financial information, purchase history or other business data), the data is to be encrypted, marked confidential and transmitted only in approved secure methods.

Encryption and file transfer protocol (FTP)/secure file transfer protocol (SFTP): Encrypted data must be transferred using Secure FTP for critically sensitive information. Traditional FTP is used in limited cases. When encrypting, only standard proven algorithms such as advanced encryption standards (AES), International Data Encryption Algorithm (IDEA) and Rivest, Shamir, and Adelman (RSA) should be used. Pretty Good Privacy (PGP) encryption, which engages a combination of IDEA and RSA may be used. Symmetric cryptosystem key lengths must be at least 56 bits. Aside from PGP, CCC also accepts WinZip, presuming that the 128 or 256-bit AES encryption is engaged. Other options of archiving that they can receive include WinZip, WinRAR, GZIP, STUFFIT, and 7-ZIP, presuming that they are encrypted as well. They do not recommend sending Confidential Information - especially customer data - to CCC via e-mail. However, if e-mail is the only capability available, then in those limited cases, customers must encrypt the file with a strong password. Regardless of transmittal method, passwords are never to be delivered with the file. Best practice is to call the recipient and provide the password verbally (not via voice-mail).

Alternate Secure Delivery Methods: Some clients and vendors utilize secure web portals to transmit data files. Such portals must utilize Hypertext Transfer Protocol Secure (HTTPS) connections (also called Hypertext Transfer Protocol Secure (HTTP) over transport security layer (TLS), HTTP over secure socket layer (SSL), and HTTP Secure). HTTPS provides authentication of the website and associated web server with which one is communicating. The password component of the credentials to access the portal should be strong in nature (meet length requirements and complexity requirements such as case, numerals, and special characters). The password should also be communicated to CCC, or other customers/vendors separate from the web address and USER-ID, in a secure manner such as via phone. If it is customer preference that CCC utilize such a portal, then you are responsible for ensuring that the security of said portal meets or exceeds these requirements, or other secure requirements that customer organizations have determined to be appropriate.

Separation of Data Assets: Whether SFTP or secure web portals are used, physical folder separation must exist whereas other external parties have no access or visibility into CCC related assets.

All backed up network data, whether in transit or at rest is AES-256 bit encrypted.

IPS sensors and alerting are engaged.

Automated Alert Notifications are sent via text to smart phone and/or via e-mail for many conditions including:

- Server unresponsive
- Disk Space below acceptable thresholds on any given drive
- If logging software (ADAuditPlus) gets turned off or if it cannot reach a given server
- If a backup fails

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the CCC policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any CCC team member.

Physical Security

Data Center and IT Support:

For scalability and maximum security, CCC utilizes 365 Data Centers, as their colocation partner to host their in-scope system and supporting infrastructure in their enterprise-class Tier III rated data center located at 500 Commack Rd in Commack, New York. As such, 365 Data Centers is responsible for the physical security controls for the in-scope system. Please see the "Subservice Organizations" section below for a detailed listing of controls owned by the 365 Data Centers.

Logical Access

FBS is responsible for the logical security controls for the in-scope operating system, database, and application. Please see the "Subservice Organizations" section below for a detailed listing of controls owned by the FBS.

CCC Systems:

Each employee workstation and server are password protected using mixed case strong non-re-useable alphanumeric passwords, minimum length 10 characters and requires new passwords to be instituted every 30 days. A user cannot change his/her password more than once within 24 hours. A password cannot be the same as any of the last 12 passwords. It cannot contain account or full name. It must contain at least three of the four character groups: English upper-case characters (A-Z); English lowercase characters (a-z); Numerals (0 through 9); Non-alphabetic characters (i.e. !, \$, #, %). Passwords are not visible when entered and are stored in an encrypted format.

Miss-typing of passwords results in user lock-out. Users now have the ability to securely unlock themselves via the Manage Engine's active directory (AD) Self Service Plus tool. Entry to the network requires two factor authentication. Transmission Control Protocol (TCP)/internet protocol (IP) is the networking protocol, while file transfers use encryption and SFTP. Keyboard, Video (monitor), Mouse. (KVM) switching, SMTP filtering, virus protection and firewall technology all help make their encrypted virtual private network (VPN) and service network secure. CCC does not allow Wireless Fidelity (WIFI) into their office network.

Classification:

Their asset policy classifies Information into six security levels: (1) Public, (2) Internal, (3) Restricted/Internal, (4) Confidential/Internal, (5) Confidential/External and (6) Classified/External. Access to Information is determined by classification level as follows:

- Public (level 1): This Information is suitable for public dissemination. Examples include public web pages, newsletters, press releases, marketing material, etc.
- Internal (level 2): This Information could be made available to all employees of CCC primarily for the purpose of conducting company business. Examples include employee phone directory, employee handbook, general company procedures, etc. While most of these materials are not intended to be shared externally, CCC would not anticipate that their release has the potential to cause more than minor inconvenience or embarrassment
- Restricted/Internal (level 3): Restricted/Internal Information includes information that individuals or units may, with proper authority, share with other parties for the purpose of collaboration, planning, product development or sales. Examples include, but are not limited to product demonstrations, proprietary methodology, best practice recommendations and research data. Examples could also include more specialized procedures, general system configurations such as password rules and certain logs that may contain sensitive information but not to the extent that systems can be breached, or credentials can be accessed. Loss of this information could cause harm to CCC's competitive positioning but would not violate their obligation under law or third-party non-disclosure agreements
- Confidential/Internal (level 4): Human Resource, payroll and other records or data protected under local, state, federal or HIPAA regulations. The executive vice president (EVP) or Principals may also designate other internal items as Confidential/Internal in cases where unauthorized release has a higher likelihood of causing significant damage to CCC. Examples include security incident logs, financial statements, detailed network diagrams, firewall configurations and passwords. Access to Confidential/Internal materials are generally stored in secure physical locations or restricted access folders and only shared on an as-needed basis with proper approval by CCC's Human Resource Director, EVP or Principals, whose authority to grant such access varies by item. For example, the human resources (HR) Director may have the authority to share personnel details during a retirement plan audit but would not have the authority to share CCC's firewall settings

- Confidential/External (level 5): Confidential/External Information includes PII, and related data owned by clients and vendors outside of CCC for which the company acts as a custodian. Examples include client customer names & addresses, social security numbers, demographic/firmographic data, financial information and purchase history or other business data (transactional or otherwise) that CCC may incorporate into a client's marketing database or other use for other project processing. Confidential information is typically non-public information about people and what they have done. Information governed under Federal, or State disclosure statutes is classified as Confidential/External. Data owner grants access to confidential information to data users (like CCC), however data users are not allowed to disseminate this confidential information outside of non-disclosure agreements or without instructions from their clients/data owners. Unauthorized release or loss of confidential information could reasonably be expected to cause legal and/or financial consequences
- Classified/External (level 6): A limited sub-set of Confidential/External information is further defined as Classified. This level of classification may be assigned to data handled under certain government contracts or other high-security engagements. Only the EVP or chief executive officer (CEO) may define data as Classified and in doing so, may establish additional data access restrictions and employee background checks

Access privileges are restricted by user to specified servers and folders to protect customer data. Multi-tiered permission levels are assigned in their web portals. Web access is monitored. Network audit trails detail logins of all users to the system and logs duration and usage. All Microsoft products track, and display users and dates modified, etc.

All files leaving the CCC facility are encrypted, and they offer secure FTP when exchanging critically sensitive data. Traditional FTP is used in limited cases. The encryption method used is Linux Unified Key Setup (LUKS). CCC only uses standard proven algorithms such as AES, IDEA and RSA as the basis for the encryption. They most commonly use PGP, which engages a combination of IDEA and RSA. Symmetric cryptosystem key lengths must be at least 56 bits. Aside from PGP, CCC also allows WinZip, which offers 128 or 256-bit AES encryption. For files destined to CCC, they have flexibility in what they can receive including WinRAR, GZIP, STUFFIT, and 7-ZIP. Upon request, client files at rest will remain encrypted.

System Protection for E-mailed Links

Mal intended parties have been known to use web addresses in e-mails to lure unsuspecting recipients to sites that contain malware, which can result in data theft or loss. To reduce CCC's risk from this possibility, they have installed Barracuda Essentials to guard against malicious attacks that can occur when employees click on e-mail links. Barracuda Essentials scans each website and unmask the true web address.

CCC allows their employees to click on the unmasked web address to continue to the site for minimal risk links. Barracuda will automatically deny access to risky sites that cannot be verified. CCC has a procedure in place where rejected Barracuda sites can be "whitelisted" if they are verified to be safe through other sources so that their team can gain access for critical business processes.

Employees Accessing the System from Outside the CCC Network are Required to use a Two-Factor Authentication System.

Aside from needing their AD credentials (with strong password), the first time out remote users are directed to a site to scan a quick response (QR) code to use as their one time password (OTP) token. On their mobile device they will download the Sophos Authenticator app. They'll then scan the QR code. From this point forward, they will go to the app every time they want to VPN into the network where they will get a 6-digit number that will be used along with their password. This code expires 30 seconds after it has been provided, and will be different every time they log in.

Who Has Access to What?

CCC's Access Control driver is a document called A 09 02 - Access Control - Audit Log - CONFIDENTIAL. Frozen versions from their current audit cycle can be found in an A 09 - Frozen Access Control Logs sub folder. Within this constantly updated document is listed every user and well over 50 points of access, whether they be Apps, network folders, facility related, web admin related, various rights, etc.

Computer Operations - Backups

CCC utilizes Datto Siris for its system backups. All servers are backed up to two Datto appliances at the 365 Data Centers in Commack, New York. These backups are full images consisting of not only data files, but also applications and Operating System images. Copies of all backups are also transmitted to Datto's data center in Reading, Pennsylvania, with yet another copy transmitted to Datto's Salt Lake City, Utah data center. Since each backup is a fully bootable virtual machine, there is no need for a conversion to occur before performing a restore. The data is always available, immediately, and securely, both on-site and off-site ("offsite" in this case refers to a secure cloud in Reading, Pennsylvania and Salt Lake City, Utah).

Backup Frequency:

As per their schedule at the time of this audit, all servers are backed up every hour between the hours of 8:00am and 7:00pm, and then again at 10:00pm and 3:00, Monday thru Friday. Additionally, they are backed up 5 times per day on Saturday and Sunday. These backups are done to two Datto appliances located at their co-lo datacenter, 365 Data Centers in Commack, New York, before propagating to the other data centers. Datto's data centers are compliant with the Service Organization Control (SOC 1/ SSAE 16 and SOC 2) reporting standards. Renowned as the predominant credential for data centers, the criteria for SOC auditing are set forth by the American Institute of Certified Public Accountants. The operational controls and activities of Datto's facilities are audited annually in order to maintain compliance.

Encryption:

All connections from a Datto Appliance to a Datto server are made over SSH/SFTP using AES 256 Bit Encryption. All servers use encrypted RAID (Redundant Array of Independent Disks) arrays that require a master password for the RAID array to be mounted. Data stored on physical disks is encrypted. Physical security: Datto uses only SAS 70 / SSAE 16 Type II certified colocation facilities for any long-term storage of customer data. Access only granted by two-factor authentication (keycard, Biometric) and on-site security is staffed 24/7/365. Software: All customer data is stored on encrypted RAID arrays. Cloud systems are monitored 24/7/365 for anomalous behavior.

Computer Operations - Availability

System Monitoring

Their systems are constantly monitored. An automatic alert from their redundant SOPHOS firewalls IPS systems is sent directly to their EVP/chief security officer (CSO) and Director of IT if any security anomalies occur. These alerts are red-flagged and sent to the e-mail inbox. In addition, the EVP/CSO regularly reviews the ManageEngine ADAuditplus dashboard and logs. The EVP/CSO reviews all internal logs including User Management (account modifications, deletions, creations), Account Lockouts, Password changes, Logon peaks, first and last logons, Domain Controller activity, user logon failures, File audit reports (folders/files read, modified, deleted, copied, moved, etc.), and more.

In August of 2021 CCC enlisted the Sophos MTR (Managed Threat Response) software/service. Other managed detection and response (MDR) services simply notify the organization of attacks or suspicious events, and it's up to the notified organization to manage things from there.

With Sophos MTR, CCC is backed by an elite team of threat hunters and response experts who take targeted actions on our behalf to neutralize even the most sophisticated threats.

Intercept X, EDR, and MTR Overview

Managed by Sophos Central (continued)

		FEATURES	INTERCEPT X ADVANCED	INTERCEPT X ADVANCED WITH MTR ADVANCED
MANAGED SERVICE	HUMAN-LED THREAT HUNTING AND RESPONSE	24/7 Lead-driven Threat Hunting		✓
		Security Health Checks		✓
		Data Retention		✓
		Activity Reporting		✓
		Adversarial Detections		✓
		Threat Neutralization & Remediation		✓
		24/7 Lead-less Threat Hunting		✓
		Threat Response Team Lead		✓
		Direct Call-in Support		✓
		Proactive Security Posture Improvement		✓

ManageEngine's ADAuditPlus sends e-mailed alerts and reports as well as dashboard reports and report generators.

For monitoring infrastructure capacity, the EVP/CSO and IT team utilize a series of tools including WINDIRSTAT, FreeSpaceThresholdAlerts, Task Manager, Windows Explorer, etc.

Change Control

FBS is responsible for the change controls for the in-scope operating system, database, and application. Please see the "Subservice Organizations" section below for a detailed listing of controls owned by the FBS.

Software Development Lifecycle (SDLC) Purpose: CCC is dedicated to maintaining strict controls regarding the request, development, quality assurance and deployment of an application. When considering a request, the requestor considers the business case, whether there is a pre-existing tool available, and the developer best suited for the request (internal or outsourced). CCC's SDLC is integrated with Change Management and Test Case policies with the lifecycle describing the steps, the Change Control Policy describing reviews, approvals, and deployment, and the Test Case Policy describing how a program's execution is validated. In order to provide a mechanism for requesting, approving and implementing changes, CCC utilizes a combination of people, procedures, and systems. The purpose of this policy is to define the flow of software development from ideation to delivery.

Policy: CCC's SDLC follows an agile methodology. The methodology has been tuned to CCC's organization, cadence and people. The steps in the life cycle are as follows:

- **General:**
 - CCC utilizes a 2 week Sprint cadence
 - Requestor: Commonly a Stakeholder or Product Owner
 - Actor: Commonly a Developer
- **Ticket Requests:**
 - All work is required to be requested and tracked in a Jira ticket

- The ticket is intended to contain the request in as much detail as available with the understanding it may be further expanded as the ticket comes to the top of the backlog for execution
- Tickets are created with acceptance criteria by the requestor:
 - Acceptance criteria outlines:
 - Inputs and desired outputs
 - Special security considerations
 - Specific test cases for validation
 - General outcomes
 - What is needed, rather than how it is to be implemented
 - In lieu of a submission by a requestor in Jira with well-defined acceptance criteria, the actor may create a placeholder ticket from discussion. In these cases, it is acknowledged by the requestor and product owner that research needed to clearly define the acceptance criteria will influence:
 - A tickets accepted into a sprint and
 - The tickets point value (and thus, time to completion)
- **Sprint Planning:**
 - Done at the beginning of each Sprint
 - In preparation of sprint planning, it is the responsibility of the Product Owner and Actors to perform regular backlog grooming to assess:
 - ROI
 - Long-term planning
 - Viability of solution
 - Grouping into actionable/measurable Epics
 - Determine what is planned to be in the next sprint via roundtable discussion with the product owner, requestor, and actor
 - The product owner is present to determine if a ticket is "worth it" based on ROI, competitive positioning and product vision
 - The requestor/stakeholder is present to provide clarification on the "what" of the ticket and to advocate for its benefit
 - The actor is present to provide an analysis of the level of effort / points, feasibility of implementation, available 3rd party tools/libraries operating/data security considerations, and timeline given their individual velocity and current set of assigned tickets
 - The ultimate takeaway of this meeting is a prioritized list of requests for the upcoming 2 weeks per developer
- **Sprint Execution:**
 - A daily scrum is used to update the team on:
 - Blockers, impediments and special items of note
 - Actions taken on the prior day
 - Planned actions for the current day
 - Callouts to in sprint request/ticket changes, bug fixes, and emergency releases
 - The Jira / Kanban Board is utilized to monitor tickets state from "To Do" → "Done"
 - To Do:
 - Work has yet to begin
 - Has been put on hold (with documentation of any impediments) OR
 - Has been returned to the Actor after not passing Peer Review
 - Next phase → "Doing" or "Done" (only via "won't do" and performed by an administrator)
 - Doing:
 - Work is actively being performed on the ticket
 - All changes are performed in isolated developer environments
 - Next phase → "To Do" or "Peer Review"
 - Peer Review:
 - Work to be reviewed
 - All changes are accessible in a testing environment

- Next Phase → “To Do” (rejected) or “Accepted”
- Accepted:
 - Work that has been reviewed by the requestor and meets requirements
 - At this stage, no code has been released to the production environment
 - Next Phase → “Done” (upon merge of code to master and release to production)
- Done:
 - All related work is in production
 - Next Phase → Archived at end of sprint or “To Do” (rare and signifies production has been rolled back)
- **Sprint Review:**
 - Developers discuss implementation and potential effects to the rest of the team
 - Demonstrations to be presented in follow-up meetings on request
 - Discussion on reporting / findings
 - Determining if follow-up meetings are needed for further exploration
 - Confirm that all tickets in “Done” with associated branches have been merged/deployed
- **Sprint Retrospective:**
 - A time for product owners, requestors, and actors to discuss:
 - Achievements
 - Doing Well
 - Could Have Done Better
 - Action items / takeaways
 - This is a blameless meeting. It is not about people as much as it is about process improvement to make things work better for the people subject to these processes / policies

Data Communications

State of the art redundant Sophos Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Network address translation (NAT) functionality is utilized to manage internal IP addresses. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes firewalls, routers, and servers. In the event that a primary system fails, the redundant hardware is configured to take its place. Firewalls at both the remote data center and their sole office located in East Islip both have built-in redundancy.

Penetration testing is conducted to measure the security posture of a target system or environment annually. The third-party vendor uses an accepted industry standard penetration testing methodology. The third-party vendor’s approach begins with a vulnerability analysis of the target system to determine what vulnerabilities exist on the system that can be exploited via a penetration test, simulating a disgruntled/disaffected insider or an attacker that has obtained internal access to the network. Once vulnerabilities are identified, the third-party vendor attempts to exploit the vulnerabilities to determine whether unauthorized access or other malicious activity is possible. After receiving the Pen Test Report, CCC with the help of FBS remediates the vulnerabilities. Then the original tester performs remediation testing to confirm that the vulnerabilities have been resolved.

External vulnerability scanning is performed on monthly basis by FBS utilizing AEGIFY scanning software. The third-party vendor uses industry standard scanning technologies and produces both a full report and then a report summary prepared by FBS. These technologies are customized to test the organization’s infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Retests and on-demand scans are performed on an as needed basis.

Authorized employees may access the system through from the Internet through the use of leading Sophos VPN technology. Employees are authenticated through the use of a token-based two-factor authentication system, which requires the use of a different unique 6-digit key generated and sent to their mobile device.

Boundaries of the System

The scope of this report includes the Data Management Solutions Services System performed in the East Islip, New York facilities.

This report does not include the colocation services provided by 365 Data Centers at the Commack, New York facilities. CCC monitors 365 Data Centers on an annual basis by collecting appropriate third-party audit document from them.

This report does not include the managed IT services provided by FBS at the Commack, New York facilities. CCC obtains and reviewed FBS' SOC report on an annual basis.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

Control Environment

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of CCC's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of CCC's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally documented organizational policy statements, codes of conduct and behavioral standards are included within the Employee Handbook
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the Employee Handbook and understand their responsibility for adhering to the policies and procedures contained within the manual
- A Non-disclosure Agreement instructing not to disclose proprietary or confidential information, including client information, to unauthorized parties is signed by each employee at hire
- A Non-Solicitation Agreement is signed at hire to protect company & client confidential information during employment and after termination
- Background checks are performed for employees as a component of the hiring process
- ISMS Risk Assessment Policy and the accompanying annual detailed Risk Assessments

Commitment to Competence

CCC's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements

- These factors are carefully considered during the interview process as well as during the reference checks
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

CCC's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Management is annually briefed on regulatory and industry changes affecting the services provided
- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole. Aside from daily 9:00 management meetings, additional meetings and steering committee gatherings occur to discuss various topics. Periodic recaps are also provided to key staff by the Principal/EVP Database Marketing

Organizational Structure and Assignment of Authority and Responsibility

CCC's organizational structure provide the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

CCC's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties.

In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed

Human Resources Policies and Practices

CCC's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. CCC's human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the Employee Handbook and Policies & Procedures Manual at hire
- New Employees are required to sign Nondisclosure and Non-Solicitation Agreements at hire
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

Risk Assessment Process

CCC is dedicated to managing risk through the implementation of, and compliance with, a comprehensive ISMS that meets ISO/IEC 27001:2013 standards. Managing risk is not a one-time event, but rather a process that requires continuous attention to monitoring and reducing risk on known items as well as identifying new areas that may involve recently evolving risks. A single data breach could have devastated impact to CCC's business in areas ranging from client loss to damaged reputation & brand value, legal costs and financial loss which may or may not be adequately covered by insurance. Adherence to this Risk Assessment Policy and the associated risk management and security procedures are considered to be of paramount importance within their organization.

All employees, vendors and systems play a role in their risk management efforts; however, this policy applies specifically to CCC's leadership team consisting of their EVP, Principals and Director of Finance/HR. Additional staff members may provide targeted input and will be looped in as needed.

No less frequently than annually, CCC will perform a complete Risk Assessment to include:

- Review prior year's risk assessment and document findings
- Assess all items with a potential to generate a future material risk and assign an owner to each
- Make a determination of which risks shall be deemed 'acceptable', which shall generally include all 'low risk' items. Select moderate and higher risk items may be designated as 'acceptable' for an upcoming year provided reasoning is provided:
 - In addition to other risks as may be deemed appropriate to measure, the CEO and EVP are required to both review every ISO-IEC 27001-2013 Clause/Annex and come to consensus on meeting each requirement. Such status is to be noted directly into a master excel listing all annex/clauses and shall include all cross-referenced policies and attachments that are relevant to the item in question. Any non-conformities must be noted with a remediation plan or explanation as to why it is acceptable. Requiring both the CEO and EVP to review and sign-off on each item helps ensure non-conflict and facilitate a fair and accurate assessment
- For those risks not deemed 'acceptable', define reduced risk targets with high-level guidance as to how such reduction may be achieved. Focus should also be placed on keeping those items with 'acceptable risk' designations at or below defined risk levels
- Create an A-CAT strategy for each item:
 - Avoid Risk: Change plans to circumvent the problem
 - Control/Mitigate Risk: Take steps to reduce the impact or likelihood
 - Accept Risk: Take the chance of negative impact and budget the cost
 - Transfer Risk: to third parties that can manage the outcome; either financially through insurance or operationally through outsourcing
- Secure sign-off on final Risk Assessment by key stakeholders
- Communicate findings and go-forward assignments to staff as appropriate
- Retain documentation of Risk Assessment

To facilitate this effort, the stakeholders shall utilize metrics defined in Master Risk Assessment workbook, which includes a 15-point scale for each of four categories: (1) Probability of Occurrence; (2) Probability of Non-Recovery; (3) Cost of Recovery; and (4) Cost of Non-Recovery. An average will be taken for a final score which translates to a risk level.

CCC's EVP shall be responsible for managing this process. Oversight of the process is provided by CEO.

Any personnel found to have violated this procedure will be subject to disciplinary action including, but not limited to training, demotion or termination.

This policy will be reviewed and updated as needed, at minimum, on an annual basis. Formal reviews and changes made to the policy must be logged below and approved by the CEO.

Information and Communications Systems

Information and communication are an integral component of CCC's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At CCC, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

There are several types of scheduling and tracking systems that their employees engage with on a daily basis. The first is "Job Tracker", where employees account for their full day by recording Clients, Project Numbers, specific Task, notes, and hours/minutes spent on each. It allows management to understand who is doing what and lends insight into client profitability. It also is utilized for Attendance recording/payroll. The "Production Schedule" lists all completed, pending, and In Progress campaigns, database updates, and projects. Contains clients, project numbers, project descriptions, A/E and Production Programmer assignment, relevant dates, and daily status, as provided by both A/E's and Production Programmers.

Application Development projects are managed via 2-week sprints and tracked by the JIRA project management system. Sprint planning meetings are held every other Monday and followed by on the Wednesday of that week the full blown sprint meeting attended by all developers, their management, executive management, and stakeholders.

- All requests for changes to the environment, as outlined above, will require a request submitted to the Jira ticketing system. The request will include the following elements:
 - Requestor name
 - Actor name
 - Reviewer name
 - Component (generally the related Bitbucket repository or project)
 - Detailed description of the change request
 - Date the change is requested
 - Priority (low, medium, high, critical)
 - Testing required (if applicable / atypical)
 - Rollback procedure (if applicable / atypical)
 - Story point estimate
- Once submitted, the change will be assigned to one of the following Jira queues, depending on priority:
 - Backlog (for prioritization at a later time)
 - A specific sprint and assignee (for more pressing needs)
 - Given the urgent nature of a substantial part of CCC business needs, tickets brought into an active sprint are expected and accepted
- Following the SDLC process, once a ticket has been accepted into an active sprint, code changes will utilize the following tools and processes to ensure proper Change Management while still allowing for rapid releases and:
 - To Do:
 - Doing
 - Peer review
 - Accepted
 - Done
- During implementation and Peer Review, the actor and reviewer are responsible for ensuring:
 - Best practices for stability, security, and monitoring are implemented to a suitable degree using the OWASP Secure Coding Practices and SANS Top 25 Programming Errors as guides
 - All operations outside of CCCs VPN are performed in a manner consistent with the DMO New Security Summary
 - Within reason, programs fail gracefully, and errors are logged
 - If required, vulnerability scanning is executed
 - All unit, integration, and regression tests pass under acceptable thresholds

- Test data remains secure and anonymized where applicable
- Dependency maintenance is routinely checked and outdate libraries are updated
- 3rd party library manipulations are non-existent
- Any applicable documentation including system topology, network configuration and application architecture will be updated. These will remain right sized to the applicable individual/role.
 - Developer notes will exist as comments within the code that can be exported via a documentation library
 - End User notes will be maintained in Confluence and regularly exported as Word/PDF documents for full company release
 - Any documents created by other proprietary systems will also be saved in a standardized format (PDF, Word, Excel, Markdown) in the case that a service is deprecated or inaccessible
- All development is to be performed on designated systems, including those:
 - Within CCCs VPN
 - Accepted services (AWS, Databricks, etc.)
 - Specific individual computers allowed by CCC management (with the strict exclusion of sensitive data)
- Production and test environments are to have strict access policies in which deployed code is executable by users and writable only by developers
- All repositories in Bitbucket are to maintain a quarterly backup in AWS S3

Daily 9:00 Management calls take place with representatives of Executive Management, Account Services, Production Programming, and Application Development. Weekly Departmental meetings are held for both Account Services and Production Programming.

Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. CCC's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

CCC's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings and walkthroughs, reviews of network project folders, tracking of quality control. Incidents and remediation, the review of system generated reports, the monitoring is constant.

Management's close involvement in CCC's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. Corrective actions, if necessary, are documented and tracked within the internal tracking log. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

HIPAA/HITECH REQUIREMENTS AND RELATED CONTROLS

Periodic Assessments

CCC has a risk assessment process in place to identify and manage the risks that could affect the Company's ability to provide services to its user entities. The risk assessment procedure defines the responsibility, methodologies and processes used by CCC to assess the risks while providing services and develop mitigation strategies to address those risks. This process requires the Company to identify risk based on management's internal knowledge of its operations. The following risk factors are discussed among the executive management including the CEO and Executive Vice President and Chief Security Officer at periodic intervals:

- *Risk Assessment:* The risk assessment is performed by the risk management personnel. Risk factors associated with the delivery or implementation of services to customers are evaluated considering process owners, dependencies, timelines and quality
- *Health Information Security Risks:* Health information security risks are assessed by the CEO and Executive Vice President and Chief Security Officer. Risk factors associated with the organization are evaluated considering compliance obligations, laws and regulations, policies and procedures, contracts and best practices to which the organization has committed to. Information security assessments carried out by risk management personnel are rolled up to the CEO and Executive Vice President and Chief Security Officer of the organization

Policies and Procedures

Health information security policies and procedures have been implemented regarding the protection of information assets. The policies and procedures act as a guide for all CCC personnel. These policies and procedures define guidelines for the health information security program related to scope of services, which includes implementing and managing logical access security and controls, including the following:

- Health information security policy
- Asset management
- Data classification
- Business continuity
- Incident management
- Access control
- Physical security

These policies are reviewed and approved by management on at least an annual basis.

Security Awareness Training

CCC employees receive security awareness training for health information security as part of the onboarding process. This training is reinforced by security awareness communications on current issues which are distributed periodically. Additionally, employees are also required to participate in annual security awareness training.

Periodic Testing and Evaluation

CCC completes evaluations throughout each calendar year regarding the effectiveness of the health information security program that include, but are not limited to, the following:

- Internal risk assessments
- Corrective action plans
- Management reviews

Remediation and Continuous Improvement

Areas of non-compliance in CCC's internal control system surface from many sources, including the Company's ongoing monitoring procedures, separate evaluations of the internal control system, and external parties. Management has developed protocols to help ensure findings, if identified, of internal control non-compliant items should be reported not only to the individual responsible for the function or activity involved, who is in the position to take corrective action. This process enables that individual to provide needed support or oversight for taking corrective action, and to communicate with others in the organization whose activities may be affected. Management evaluates the specific facts and circumstances related to areas of non-compliance in internal control procedures and make the decision for addressing any non-compliant items based on whether the incident was isolated or requires a change in the Company's procedures or personnel.

Incident Response

CCC maintains a documented incident response plan including breach notification requirements as mandated by HITECH. The procedures include, but are not limited to, the identification, response, escalation, and remediation of security breaches and other incidents. A formal breach notification process is utilized to document and track resolution of incidents noted. The incident response procedures are tested during the normal course of business and are updated as needed.

Changes to the System Since the Last Review

No significant changes have occurred to the services provided to user entities since the organization last review.

Incidents Since the Last Review

No significant incidents have occurred to the services provided to user entities since the organization last review.

Trust Services Criteria and HIPAA/HITECH Requirements Not applicable to the System

The following criteria and requirements were Not applicable to the system:

Requirements Not applicable to the System		
Criteria / Safeguard	Requirement	Reason
Administrative Safeguard	164.308(a)(4)(ii)(A)	The entity is not a healthcare clearinghouse.
Physical Safeguard	164.310(c)	The entity is not a covered entity.
Organizational Safeguard	164.314(a)(2)(ii)	The entity is not a government entity.
	164.314 b)(1), 164.314(b)(2)	The entity is not a plan sponsor.

Requirements Not applicable to the System		
Criteria / Safeguard	Requirement	Reason
Breach Safeguard	164.404(a), 164.404(b), 164.404(c)(1), 164.404(c)(2), 164.404(d)(1)(i), 164.404(d)(1)(ii), 164.404(d)(2), 164.404(d)(2)(i), 164.404(d)(2)(ii), 164.404(d)(3), 164.406, 164.408(a), 164.408(b), 164.408(c)	The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

Subservice Organizations

This report does not include the colocation services provided by 365 Data Centers at the Commack, New York facilities.

This report does not include the managed IT services provided by FBS at the Commack, New York facilities.

Subservice Description of Services

365 Data Centers is a leading provider of cloud, connectivity, and data center services for enterprise, carrier, and content customers. In addition to security, their contract also ensures uptime through multiple levels of redundancy. The Data Center has received accolades and awards for outstanding IT services and support and key considerations include:

Power

- Underground 13.2k primary service
- Total isolation A & B power distribution paths
- Individual long time, short time, instantaneous and ground fault (LSIG) breaker micro-logic trip units, providing fault isolations
- Electronic transfer switching, using Payment Card Industry (PCI) logic controls
- Individual branch breaker isolation and reporting capabilities

Backup Emergency Power

- N+ 1 generators that exceeds continuous Tier III rating standards
- Designed not to limit consecutive hours of operation when commercial utility is disrupted
- Redundant fuel pumping system from primary underground fuel storage tank to reserved installed day tanks on each unit; providing N+1 system

Fuel Capacity

- 125 hours (5+ days) of onsite fuel storage (at full load). Far exceeding Tier III standards
- Sophisticated fuel polishing system, maintaining proper nutrients, eliminating all containments, fuel breakdown, and moisture buildup
- Multiple fuel vendor contracts for fuel delivery services

Mechanicals

- 2N redundant cooling system
- Highly efficient cooling system using economization technology, providing six-eight month 'free cooling' mode. (Full economization = the economizer is handling the load with no compressor power, thus reducing overall costs and increasing efficiency levels)

Fire Protection

- FFAST Air Sampling Technology - (Fire Alarm Aspiration Sensing Technology)
- Technology uses an advanced, intelligent smoke detector that actively draws air into its sensors for early warning detections
- Clean agent gas FK-5-1-12 aka Novec1230 Sapphire
- System designed as 'Main/Reserve' throughout datacenter & Power Rooms
- Lowest environmental impact of all the chemical clean agents

Monitoring

- Fully functional Building Management System (BMS), coupled with enterprise Emergency Power Monitoring System (EPMS) offers total visibility at every component layer of the electrical and mechanical infrastructure
- Built-in intelligence to respond to conditions and turn on and off redundant mechanical systems
- Hi-Tech dashboard visuals, with advanced smartphone alerting capability
- Completion visualization of power devices; tracking, recording, and reporting advanced technology to report on volts/amps to lower branch breaker layer

Security

- Advanced physical security systems, combined with 365 Data Centers access policies offer customer confidence and peace of mind
- Dual authentication security checkpoints at critical entrance locations
- Innovative, secured customer cabinets offer alerting, tracking and recording functionality and remote notifications as an option
- Video surveillance complying with PCI standards

FBS provides IT management services. These services include technology planning, implementation, access management, change management, and other peripheral IT needs.

Complementary Subservice Organization Controls

CCC's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called subservice organization controls. It is not feasible for all of the trust services criteria related to CCC's services to be solely achieved by CCC control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of CCC.

The following subservice organization controls should be implemented by 365 Data Centers to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - 365 Data Centers		
Category / Safeguard	Criteria / Requirement	Control
Security / Common Criteria	CC6.4, 164.310(a)(1), 164.310(a)(2)(ii), 164.310(a)(2)(iii), 164.310(a)(2)(iv)	Physical access controls are in place to restrict access to and within the data center facilities.
		Physical access requests are documented and require the approval of the site manager.
		A review of Digital Realty employees and contractors with physical access to customer suites is performed on a quarterly basis and unnecessary access is identified, modified, and removed as necessary.
		A termination notification is completed by HR and physical access is revoked by the corporate security team for Digital Realty employees and contractors within one business of termination.
		Visitors are required to surrender their badges upon exit. Access badges for visitors that do not require an escort are configured to expire at the end of the day.
		Surveillance cameras are in place to monitor and record access to and within the data centers. Surveillance cameras are located along the building perimeters and within the data centers.
		Digital surveillance systems are configured to retain video footage for the data centers for a minimum of 90 days.
Availability	A1.2	Environmental protections of systems at the data center are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.

The following subservice organization controls should be implemented by FBS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - FBS		
Category / Safeguard	Criteria / Requirement	Control
Common Criteria / Security	CC6.1, CC6.3	Operating system user access is restricted via role based security privileges defined within the access control system.
		Operating system administrative access is restricted to user accounts accessible by authorized personnel.

Subservice Organization - FBS		
Category / Safeguard	Criteria / Requirement	Control
		Operating systems are configured to enforce password requirements that include: <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity
		Operating system users are authenticated via individually-assigned user accounts and passwords.
		Operating system account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset
		Operating system audit logging settings are in place that include: <ul style="list-style-type: none"> • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events
		Operating system audit logs are maintained and reviewed as-needed.
		Database user access is restricted via role based security privileges defined within the access control system.
		Database administrative access is restricted to user accounts accessible by authorized personnel.
		Databases are configured to enforce password requirements that include: <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity
		Database users are authenticated via individually-assigned user accounts and passwords.

Subservice Organization - FBS		
Category / Safeguard	Criteria / Requirement	Control
		Database account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset
		Application user access is restricted via role based security privileges defined within the access control system.
		Application administrative access is restricted to user accounts accessible by authorized personnel.
		The application is configured to enforce password requirements that include: <ul style="list-style-type: none"> • Password history • Password age • Password length • Complexity
		Application users are authenticated via individually-assigned user accounts and passwords.
		Application account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset
		Application audit policy settings are in place that include: <ul style="list-style-type: none"> • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events
		Application audit logs are maintained and reviewed as-needed.
Common Criteria / Security	CC7.2	Operating system account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset

Subservice Organization - FBS

Category / Safeguard	Criteria / Requirement	Control
		Operating system audit logging settings are in place that include: <ul style="list-style-type: none"> • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events
		Operating system audit logs are maintained and reviewed as-needed.
		Database account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset
		Database audit logging settings are in place that include: <ul style="list-style-type: none"> • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events
		Database audit logs are maintained and reviewed as-needed.
		Application account lockout settings are in place that include: <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Account lockout counter reset

Subservice Organization - FBS		
Category / Safeguard	Criteria / Requirement	Control
		Application audit policy settings are in place that include: <ul style="list-style-type: none"> • Account logon events • Account management • Directory Service Access • Logon events • Object access • Policy changes • Privilege use • Process tracking • System events
		Application audit logs are maintained and reviewed as-needed.
Common Criteria / Security	CC8.1	Operating system, infrastructure, and database changes are communicated to both affected internal and external users.
		Operating system, infrastructure, and database changes are tested prior to implementation. Types of testing performed depend on the nature of the change.
		Operating system, infrastructure, and database changes are authorized and approved by management prior to implementation.

CCC management, along with the subservice organizations, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, CCC performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations
- Reviewing attestation reports over services provided by vendors and subservice organizations
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organizations

COMPLEMENTARY USER ENTITY CONTROLS

CCC's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria and HIPAA/HITECH requirements related to CCC's services to be solely achieved by CCC control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of CCC's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria and HIPAA/HITECH requirements described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls:

1. User entities (clients of CCC) are responsible for advising the service organization (CCC) of the termination or status change of an employee who possesses the credentials to access CCC's systems including CCC's SFTP, CrossSelect or APEARS sites, or of any off-cycle necessity to change credentials. CCC may have no way of knowing when a user entity's access should be removed and needs to be advised in order to change the credentials or adjust IP whitelisting.
2. User entities are responsible for maintaining their own system(s) of record.
3. User entities are responsible for advising the service organization of the termination or status change of an employee or other agent who is authorized to provide instructions to CCC, or who is on any distribution lists for the purpose of receiving reports and/or communications.
4. User entities are responsible for understanding and complying with their contractual obligations to CCC.
5. User entities are responsible for adhering to best practices on secure transmission of confidential or PII.
6. User entities are responsible for advising CCC of any changes to file formats, valid data values, or processing instructions.
7. User entities are responsible for ensuring their own compliance with any applicable laws, regulations, privacy policies or best practices and to ensuring that any provided data/instructions to CCC (or requests of CCC) would be consistent with User Entities own obligations. With regard to General Data Protection Regulation (GDPR), the User Entity is considered the Controller and the service organization (CCC) is considered the Processor.
8. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize CCC services.
9. User entities are responsible for immediately notifying CCC of any actual or suspected information security breaches, including compromised user accounts, including those used for online access and secure file transfers.

TRUST SERVICES CATEGORIES

In-Scope Trust Services Categories

Common Criteria (to the Security, Availability, and Confidentiality Categories)

Security refers to the protection of

- i. information during its collection or creation, use, processing, transmission, and storage and
- ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

HEALTH INFORMATION SECURITY PROGRAM

CCC has developed a health information security management program to meet the information security and compliance requirements related to Data Management Solutions Services System and its customer base. The program incorporates the elements of the HIPAA and the HITECH. The description below is a summary of safeguards that CCC has implemented to adhere to the applicable components of HIPAA Final Security Rule and the breach notification requirements of HITECH.

Administrative Safeguards - Policies and procedures designed to show how CCC complies with the act:

- Management has adopted a written set of health information security policies and designated the information security officer to be responsible for developing and implementing the required policies and procedures.
- Procedures address access authorization, establishment, modification, and termination.
- Documented incident response policies for reporting security incidents are in place to guide employees in identifying, reporting, of security incidents.
- Business continuity plans are documented to enable continuation of critical business processes in the event of an emergency.
- Privileged administrative access to systems is restricted to authorized individuals.
- Automated backup systems are in place to perform scheduled replication of production data and systems at pre-defined intervals.
- Antivirus software is utilized to detect and eliminate data or files that contain certain virus signatures on certain production servers.

Physical Safeguards - Controlling physical access to protected data:

- Documented physical security policies and procedures are in place to guide personnel in physical security administration.
- Physical access procedures are in place restrict access, log visitors, and terminate access to the office facility.
- Inventory listings are utilized to track and monitor hardware and removable media.
- Data destruction procedures are in place to guide the secure disposal of data and media.

Technical Safeguards - Controlling access to computer systems and enabling covered entities to protect communications containing PHI transmitted electronically over open networks from being intercepted by anyone other than the intended recipient:

- Access to in-scope systems is restricted to authorized personnel based on a valid user account and password.
- Systems are configured to enforce pre-determined thresholds to lock user sessions due to invalid login attempts.
- Security monitoring applications and manual reviews are utilized to monitor and analyze the in-scope systems for possible or actual security breaches.

Organizational Requirements - Adherence to policies and procedures in regard to PHI documentation availability, as well as documentation retention:

- Documented policies address the confidentiality threshold of PHI documents and the length of time they should be retained before being destroyed.
- Contractual responsibilities by subparts of an organization are written and maintained in contracts.
- Separation of duties is existent in order to protect to confidentiality, availability, and integrity of PHI.
- Ensure that only appropriate parties gain access to PHI internally and external to the organization.

Breach Notification - A business associate shall, following the discovery of a breach of unsecured PHI, notify the covered entity of such breach:

- Documented policies and procedures are in place to guide personnel in notifying the covered entity upon discovery of a breach.
- Documented policies and procedures are in place to guide personnel in responding to discovery of a breach.
- Documented policies and procedures require disclosure of the unsecured PHI and include, to the extent possible, the identification of each individual and a description of the event.
- Documented policies and procedures are in place to guide personnel in the exception processes of delaying and documenting notifications.
- Documented policies and procedures are in place to guide personnel in documentation of administrative requirements for demonstrating that all notifications were made as required.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	Control Environment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	<p>Core values are communicated from executive management to personnel through policies, directives, guidelines, the code of conduct and the employee handbook.</p> <p>An employee handbook and code of conduct are documented to communicate workforce conduct standards and enforcement procedures.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.</p> <p>Upon hire, personnel are required to sign a non-disclosure agreement.</p> <p>Prior to employment, personnel are required to complete a background check.</p> <p>Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.</p> <p>Performance and conduct evaluations are performed for personnel on an annual basis.</p> <p>Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.</p> <p>Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.</p>
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	<p>Executive management roles and responsibilities are documented and reviewed annually.</p> <p>Executive management defines and documents the skills and expertise needed among its members.</p> <p>Executive management evaluates the skills and expertise of its members annually.</p> <p>The entity performs an internal assessment of the controls environment annually to assess the effectiveness of controls within the environment.</p> <p>Executive management maintains independence from those that operate the key controls within the environment.</p> <p>Executive management meets annually with operational management to assess the effectiveness and performance of internal controls within the environment.</p> <p>Executive management evaluates the skills and competencies of those that operate the internal controls within the environment annually.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	Control Environment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	<p>Operational management assigns responsibility for and monitors the effectiveness and performance of internal controls implemented within the environment.</p> <p>A third-party performs an independent assessment of the entity's controls environment annually to assess the effectiveness of internal controls within the environment.</p> <p>A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.</p> <p>Executive management reviews the organizational chart annually and makes updates to the organizational structure and lines of reporting, if necessary.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p> <p>Executive management has established proper segregations of duties for key job functions and roles within the organization.</p>
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	<p>A vendor risk assessment is performed on an annual basis which includes reviewing the activities performed by third parties.</p> <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Performance and conduct evaluations are performed for personnel on an annual basis.</p> <p>The entity evaluates the competencies and experience of candidates prior to hiring.</p> <p>The entity has a recruiting department that is responsible for attracting individuals with competencies and experience that align with the entity's goals and objectives.</p> <p>Employees are required to attend continued training annually that relates to their job role and responsibilities.</p> <p>Executive management has created a training program for its employees.</p> <p>The entity assesses training needs on an annual basis.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC1.0	Control Environment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	<p>Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance.</p> <p>Prior to employment, personnel are required to complete a background check.</p> <p>A documented organizational chart is in place that defines organizational structures, lines of reporting, and areas of authority.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p> <p>Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.</p> <p>Policies and procedures are in place that outline the performance evaluation process as well as the competency and training requirements for personnel.</p> <p>Performance and conduct evaluations are performed for personnel on an annual basis.</p> <p>Executive management reviews the responsibilities assigned to operational personnel annually and makes updates, if necessary.</p> <p>Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC2.0	Information and Communication	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	<p>Organizational and information security policies and procedures are documented for supporting the functioning of controls and processes and made available to its personnel through the entity's shared drive.</p> <p>Edit checks are in place to prevent incomplete or incorrect data from being entered into the system.</p> <p>Data flow diagrams and process flowcharts are documented and maintained by management to identify the relevant internal and external information sources of the system.</p> <p>Data processed within the system is reviewed for completeness and accuracy.</p> <p>Data output from the system is reviewed for completeness and accuracy.</p> <p>Data that entered into the system, processed by the system and output from the system is protected from unauthorized access.</p> <p>Data and information critical to the system is assessed as-needed for relevance and use.</p> <p>Data is only retained for as long as required to perform the required system functionality, service or use.</p>
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	<p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.</p> <p>The entity's policies and procedures, code of conduct and employee handbook are made available to employees through the entity's shared drive.</p> <p>Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook and code of conduct.</p> <p>Personnel are required to acknowledge the employee handbook and code of conduct on an annual basis.</p> <p>Upon hire, personnel are required to acknowledge the employee handbook which requires adherence to the personnel's job role and responsibilities.</p> <p>Executive management meets quarterly with operational management to discuss the entity's objectives as well as roles and responsibilities.</p> <p>Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC2.0	Information and Communication	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<p>Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance.</p> <p>Management tracks and monitors compliance with information security and awareness training requirements.</p> <p>The entity's third-party agreement delineates the boundaries of the system and describes relevant system components.</p> <p>The entity's third-party agreement communicates the system commitments and requirements of third parties.</p> <p>The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties.</p> <p>Customer commitments, requirements and responsibilities are outlined and communicated through service agreements.</p> <p>Changes to commitments, requirements and responsibilities are communicated to third parties, external users, and customers via mass notifications.</p> <p>Documented escalation procedures for reporting failures incidents, concerns and other complaints are in place and shared with external parties.</p> <p>Executive management meets annually with operational management to discuss the results of assessments performed by third parties.</p> <p>Employees, third parties, and customers are directed on how to report unethical behavior in a confidential manner.</p> <p>The entity communicates to external parties, vendors and service providers the system commitments and requirements relating to confidentiality through the use of third-party agreements.</p> <p>Changes to commitments and requirements relating to confidentiality are communicated to third parties, external users, and customers via mass notifications.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	Risk Assessment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	<p>The entity establishes organizational strategies and objectives that are used to determine entity structure and performance metrics.</p> <p>Executive management has documented objectives that are specific, measurable, attainable, relevant and time-bound (SMART).</p> <p>Executive management identifies and assesses risks that could prevent the entity's objectives from being achieved.</p> <p>Executive management reviews policies, procedures and other control documents for alignment to the entity's objectives on an annual basis.</p> <p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p> <p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Responsible parties are defined and assigned to coordinate and monitor compliance and audit activities.</p> <p>Executive management has established key performance indicators for operational effectiveness.</p> <p>Business plans and budgets align with the entity's strategies and objectives.</p> <p>Entity strategies, objectives and budgets are assessed on a quarterly basis.</p> <p>The entity's internal controls framework is based on the SOC framework.</p> <p>The entity undergoes compliance audits annually to show compliance to relevant laws, regulations and standards.</p>
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	<p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.</p> <p>A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	Risk Assessment	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	<p>The entity's risk assessment process includes:</p> <ul style="list-style-type: none"> • Avoiding risks • Controlling and mitigating risks • Accepting risks • Transferring risks <p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p> <p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>For gaps and vulnerabilities identified from the risk assessment, remediation efforts, including the implementation of controls, are assigned to process owners based on roles and responsibilities.</p> <p>The annual comprehensive risk assessment results are reviewed and approved by appropriate levels of management.</p> <p>As part of the annual risk assessment, management reviews the potential threats and vulnerabilities arising from its customers, vendors and third parties.</p> <p>On an annual basis, management identifies and assesses the types of fraud that could impact their business and operations.</p> <p>Identified fraud risks are reviewed and addressed using one of the following strategies:</p> <ul style="list-style-type: none"> • Avoid the risk • Mitigate the risk • Transfer the risk • Accept the risk <p>As part of management's assessment of fraud risks, management considers key fraud factors such as incentives, pressures, opportunity for unauthorized access or use of data, and employee morale and attitude.</p> <p>As part of management's assessment of fraud risks, management considers how personnel could engage in or justify fraudulent activities.</p> <p>As part of management's assessment of fraud risks, management considers threats and vulnerabilities that arise from the use of IT.</p>
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	<p>Changes to the business structure and operations are considered and evaluated as part of the annual comprehensive risk assessment.</p> <p>Changes to the entity's systems, applications, technologies, and tools are considered and evaluated as part of the annual comprehensive risk assessment.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC3.0	Risk Assessment	
Control Point	Criteria	Control Activity Specified by the Service Organization
		Changes in vendor and third-party relationships are considered and evaluated as part of the annual comprehensive risk assessment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC4.0	Monitoring Activities	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	<p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p> <p>Management reviews policies, procedures and other control documents for accuracy and applicability on an annual basis.</p> <p>On an annual basis, management reviews the controls implemented within the environment for operational effectiveness and identifies potential control gaps and weaknesses.</p> <p>The entity performs an internal assessment of the controls environment annually to assess the effectiveness of controls within the environment.</p> <p>Control self-assessments that include physical and logical access reviews are performed on an annual basis.</p> <p>Data backup restoration test is performed on a monthly basis.</p> <p>External vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.</p> <p>A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.</p> <p>A third-party performs an independent assessment of the controls environment annually to assess the effectiveness of controls within the environment.</p> <p>Performance and conduct evaluations are performed for personnel on an annual basis.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p> <p>A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p> <p>Evaluations are performed by individuals with sufficient knowledge of what is being evaluated.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC4.0	Monitoring Activities	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	<p>Internal audit performs control assessments on an annual basis and communicates results to the audit committee/executive management for monitoring of corrective actions.</p> <p>Senior management is made aware of high-risk vulnerabilities, deviations and controls gaps identified as part of the compliance, control and risk assessments performed.</p> <p>Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are communicated to those parties responsible for taking corrective actions.</p> <p>Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are documented, investigated, and addressed.</p> <p>Vulnerabilities, deviations and control gaps identified from the compliance, control and risk assessments are addressed by those parties responsible for taking corrective actions.</p> <p>Management tracks whether vulnerabilities, deviations and control gaps identified as part of the evaluations performed are addressed in a timely manner.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC5.0	Control Activities	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	<p>As part of the risk assessment process, controls within the environment are modified and implemented to mitigate identified vulnerabilities, deviations and control gaps.</p> <p>Controls within the environment are modified and implemented to mitigate vulnerabilities, deviations and control gaps identified as part of the various evaluations performed.</p> <p>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p> <p>Management has documented the relevant controls in place for each key business or operational process.</p> <p>Management has incorporated a variety of controls into their environment that include manual, automated, preventive, detective, and corrective controls.</p> <p>Management develops risk mitigation strategies, including the implementation of controls, to address risks identified during the risk assessment process.</p> <p>Business continuity and disaster recovery plans are developed and updated on an annual basis.</p> <p>Business continuity and disaster recovery plans are tested on an annual basis.</p>
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	<p>Organizational and information security policies and procedures are documented and made available to employees through the entity's shared drive.</p> <p>Management has documented the controls implemented around the entity's technology infrastructure.</p> <p>As part of the risk assessment process, the use of technology in business processes is evaluated by management.</p> <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Documented escalation procedures for reporting security incidents are in place to guide users in identifying and reporting failures, incidents, concerns, and other complaints.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC5.0	Control Activities	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	<p>Organizational and information security policies and procedures are documented and made available to employees through the entity's shared drive.</p> <p>Organizational and information security policies and procedures are reviewed on an annual basis by management.</p> <p>Management has implemented controls that are built into the organizational and information security policies and procedures.</p> <p>Process owners and key management are assigned ownership to each key internal control implemented within the entity's environment.</p> <p>Roles and responsibilities are defined in written job descriptions and communicated to personnel through the entity's shared drive.</p> <p>Performance of the internal controls implemented within the environment are assigned to appropriate process owners and operational personnel based on roles and responsibilities.</p> <p>Process owners and management investigate and troubleshoot control failures.</p> <p>Effectiveness of the internal controls implemented within the environment are evaluated annually.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	Logical and Physical Access	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	<p>An inventory of system assets and components is maintained to classify and manage the information assets.</p> <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p>
	Network - Active Directory (AD)	
		<p>Administrative access to the network is restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> • President/CEO • EVP/CSO • Director Applications Development <p>Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity <p>Active Directory account lockout policies are in place that include:</p> <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold
	Remote Access	
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	<p>VPN users are authenticated via username and a one-time password prior to being granted remote access to the system.</p> <p>VPN users are authenticated via multi-factor authentication (username, password, and OTP) prior to being granted remote access to the system.</p> <p>Privileged access to sensitive resources is restricted to defined user roles.</p> <p>Part of this criterion is the responsibility of the subservice organizations. Refer to the "Subservice Organizations" section for controls managed by the subservice organizations.</p> <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Logical access to systems is approved and granted to an employee as a component of the hiring process.</p> <p>Logical access to systems is revoked as a component of the termination process.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	Logical and Physical Access	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	<p>Control self-assessments that include physical and logical access reviews are performed on an annual basis.</p> <p>Data backup restoration test is performed on a monthly basis.</p> <p>Documented policies and procedures are in place regarding system settings, authentication, access, and security monitoring.</p> <p>Logical access to systems is approved and granted to an employee as a component of the hiring process.</p> <p>Logical access to systems is revoked as a component of the termination process.</p> <p>Control self-assessments that include physical and logical access reviews are performed on an annual basis.</p> <p>Data backup restoration test is performed on a monthly basis.</p> <p>Part of this criterion is the responsibility of the subservice organizations. Refer to the "Subservice Organizations" section for controls managed by the subservice organizations.</p>
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section above for controls managed by the subservice organization.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	<p>Policies and procedures are in place to guide personnel in data, hardware and software disposal and destruction.</p> <p>Policies and procedures are in place for removal of media storing critical data or software.</p>
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	<p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Externally routable IP addresses are not assigned to production processing servers. NAT functionality is utilized to manage internal IP addresses.</p> <p>Server certificate-based authentication is used as part of the SSL/TLS and VPN encryption with a trusted certificate authority.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	Logical and Physical Access	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	<p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.</p> <p>The antivirus software is configured to scan workstations in real time.</p> <p>Critical data is stored in encrypted format using software supporting the AES.</p> <p>A DMZ is in place to isolate outside access and data from the entity's environment.</p> <p>Use of removable media is prohibited by policy except when authorized by management.</p> <p>VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.</p> <p>Server certificate-based authentication is used as part of the SSL/TLS and VPN encryption with a trusted certificate authority.</p> <p>Stored passwords are encrypted.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Externally routable IP addresses are not assigned to production processing servers. NAT functionality is utilized to manage internal IP addresses.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Critical data is stored in encrypted format using software supporting the AES.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p> <p>An automated backup system is utilized to perform scheduled system backups.</p> <p>Full backups of certain application and database components are performed on an hourly basis.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC6.0	Logical and Physical Access	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	<p>Use of removable media is prohibited by policy except when authorized by management.</p> <p>External vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.</p> <p>A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.</p> <p>The antivirus software is configured to scan workstations in real time.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	System Operations	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	<p>Management has defined configuration standards in the information security policies and procedures.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Use of removable media is prohibited by policy except when authorized by management.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>External vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.</p> <p>A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.</p>
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>Policies and procedures are in place regarding detection, logging, and monitoring of unknown or unauthorized components into the environment.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p> <p>An automated backup system is utilized to perform scheduled system backups.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	System Operations	
Control Point	Criteria	Control Activity Specified by the Service Organization
		<p>Full backups of certain application and database components are performed on an hourly basis.</p> <p>IT personnel monitor the success or failure of backups and are notified of backup job status via e-mail notifications.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available.</p> <p>The antivirus software is configured to scan workstations in real time.</p> <p>Use of removable media is prohibited by policy except when authorized by management.</p>
	Active Directory	
		<p>Administrative access to the network is restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> • President/CEO • EVP/CSO • Director Applications Development <p>Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity <p>Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC7.0	System Operations	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.</p>
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	<p>Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are defined and documented.</p> <p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>Incidents are documented and tracked in a standardized ticketing system and updated to reflect the planned incident and problem resolution.</p> <p>A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.</p>
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	<p>Change management requests are opened for incidents that require permanent fixes.</p> <p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p> <p>Data backup restoration test is performed on a monthly basis.</p> <p>A security incident analysis is performed for critical incidents to determine the root cause, system impact and resolution.</p> <p>On an annual basis, preventative and detective controls are evaluated and changed as necessary.</p> <p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC8.0	Change Management	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	<p>Documented change control policies and procedures are in place to guide personnel in the change management process.</p> <p>The change management process has defined the following roles and assignments:</p> <ul style="list-style-type: none"> • Authorization of change requests - owner or business unit manager • Development - application design and support department • Testing - quality assurance department • Implementation - software change management group <p>System changes are communicated to both affected internal and external users.</p> <p>Application changes are configured to require peer review.</p> <p>Access to implement changes in the production environment is restricted to authorized IT personnel.</p> <p>Development and test environments are physically and logically separated from the production environment.</p> <p>System changes are authorized, reviewed and approved prior to implementation.</p> <p>Prior code is held in the source code repository for rollback capability in the event that a system change does not function as designed.</p> <p>System change requests are documented and tracked in a ticketing system.</p> <p>System changes are tested prior to implementation. Types of testing performed depend on the nature of the change.</p> <p>Information security policies and procedures document the baseline requirements for configuration of IT systems and tools.</p> <p>Documented change control policies and procedures are in place to guide personnel in implementing changes in an emergency situation.</p> <p>Part of this criterion is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC9.0	Risk Mitigation	
Control Point	Criteria	Control Activity Specified by the Service Organization
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	<p>Documented policies and procedures are in place to guide personnel in performing risk mitigation activities.</p> <p>Management has defined a formal risk assessment process that specifies the process for identifying internal and external threats and vulnerabilities, evaluating and addressing risks and defining specified risk tolerances.</p> <p>A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p> <p>Identified risks are rated using a risk evaluation process and ratings are approved by management.</p> <p>The entity's risk assessment process includes:</p> <ul style="list-style-type: none"> • Avoiding risks • Controlling and mitigating risks • Accepting risks • Transferring risks <p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.</p>
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	<p>Management has defined a third-party vendor risk management process that specifies the process for evaluating third-party risks based on identified threats and the specified tolerances.</p> <p>Management develops third-party risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>Identified third-party risks are rated using a risk evaluation process and ratings are approved by management.</p> <p>The entity's third-party agreement outlines and communicates the terms, conditions and responsibilities of third parties.</p> <p>Management obtains and reviews attestation reports of vendors and third parties to evaluate the effectiveness of controls within the vendor or third-party's environment.</p> <p>A vendor risk assessment is performed on an annual basis as a part of the risk assessment.</p>

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY		
CC9.0	Risk Mitigation	
Control Point	Criteria	Control Activity Specified by the Service Organization
		<p>Management has assigned responsibility and accountability for the management of risks associated with third parties to appropriate personnel.</p> <p>The entity has documented procedures for terminating third-party relationships.</p> <p>The entity's third-party agreement outlines and communicates confidentiality commitments and requirements.</p>

C1.0	ADDITIONAL CRITERIA FOR THE CONFIDENTIALITY CATEGORY	
Control Point	Criteria	Control Activity Specified by the Service Organization
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	<p>Documented confidential policies and procedures are in place that include the following:</p> <ul style="list-style-type: none"> • Defining, identifying and designating information as confidential • Storing confidential information • Protecting confidential information from erasure or destruction • Retaining confidential information for only as long as is required to achieve the purpose for which the data was collected and processed <p>An inventory log is maintained of assets with confidential data.</p> <p>Confidential information is maintained in locations restricted to those authorized to access.</p>
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	<p>Documented data destruction policies and procedures are in place that include the following:</p> <ul style="list-style-type: none"> • Identifying confidential information requiring destruction when the end of the retention period is reached • Erasing or destroying confidential information that has been identified for destruction <p>An inventory log is maintained of assets with confidential data, and as confidential data meets the retention period, the data is destroyed or purged.</p> <p>The entity retains confidential data for a period, depending on the key file types to achieve the purpose for which the data was collected and processed.</p>

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(1)(i)	Security management process: Implement policies and procedures to prevent, detect, contain and correct security violations.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity.</p> <p>The monitoring software is configured to alert IT personnel when thresholds have been exceeded.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p> <p>External vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.</p> <p>A third-party performs a penetration testing annually to identify and exploit vulnerabilities identified within the environment.</p>
164.308 (a)(1)(ii)(A)	Risk analysis: Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	<p>Documented policies and procedures are in place to guide personnel when performing a risk assessment.</p> <p>A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements.</p>
164.308 (a)(1)(ii)(B)	Risk management: Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with § 164.306(a). Factors identified in §164.306 include: <ul style="list-style-type: none"> • The size, complexity, capability of the covered entity • The covered entity's technical infrastructure • The costs of security measures • The probability and criticality of potential risks to ePHI 	<p>Management develops risk mitigation strategies to address risks identified during the risk assessment process.</p> <p>External vulnerability scans are performed monthly on the environment to identify control gaps and vulnerabilities.</p> <p>An IPS is utilized to analyze network events and report possible or actual network security breaches.</p> <p>The IPS is configured to notify personnel upon intrusion prevention.</p> <p>Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software.</p>

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(1)(ii)(C)	Sanction policy: Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	<p>A firewall is in place to filter unauthorized inbound network traffic from the internet.</p> <p>The firewall system is configured to deny any type of network connection that is not explicitly authorized by a firewall system rule.</p> <p>Sanction policies, which include probation, suspension and termination, are in place for employee misconduct.</p>
164.308 (a)(1)(ii)(D)	Information system activity review: Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p>
164.308 (a)(2)	Assigned security responsibility: Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	<p>Responsibility for the development, implementation, and regular maintenance of the policies and procedures that govern the security of protected ePHI is formally documented and assigned to the EVP and Chief Security Officer.</p>
164.308 (a)(3)(i)	Workforce security: Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under the Information Access Management standard and to prevent those who do not have appropriate access from obtaining access to ePHI. Policies and procedures should include Authorization and/or Supervision procedures, Workforce Clearance Procedure, and Termination Procedures.	<p>Privileged access to sensitive resources is restricted to defined user roles.</p> <p>Control self-assessments that include physical and logical access reviews are performed on an annual basis.</p>
164.308 (a)(3)(ii)(A)	Authorization and/or supervision: Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	<p>Documented policies and procedures are in place regarding workforce members who work with ePHI or in locations where it might be accessed.</p> <p>Standardized user access request tickets are utilized to request access to ePHI prior to access being granted.</p>
164.308 (a)(3)(ii)(B)	Workforce clearance procedure: Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	<p>Workforce members have appropriate access to ePHI.</p> <p>Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel.</p> <p>Control self-assessments that include physical and logical access reviews are performed on an annual basis.</p>

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(3)(ii)(C)	Termination procedures: Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) [the Workforce Clearance Procedure] of this section.	Termination procedures require the removal of employee access to ePHI upon termination of employment. Access to ePHI is revoked as a component of the termination process.
164.308 (a)(4)(i)	Information access management: Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of the Privacy Rule. Policies and procedures should include Isolating Health Care Clearinghouse Functions, Access Authorization and Access Establishment and Modification.	Management maintains policies and procedures that ensure the authorization of access to ePHI and are consistent with the applicable requirements of the Privacy Rule.
164.308 (a)(4)(ii)(A)	Isolating healthcare clearinghouse functions: If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	Not applicable. The entity is not a healthcare clearinghouse.
164.308 (a)(4)(ii)(B)	Access authorization: Implement policies and procedures for granting access to ePHI, for example, through access to a workstation, transaction, program, process, or other mechanism.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Standardized user access request tickets are utilized to request access to ePHI prior to access being granted.
164.308 (a)(4)(ii)(C)	Access establishment and modification: Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel. Standardized user access request tickets are utilized to request access to ePHI prior to access being granted. Access to ePHI is revoked as a component of the termination process. Control self-assessments that include physical and logical access reviews are performed on an annual basis.

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(5)(i)	Security awareness and training: Implement a security awareness and training program for all members of the workforce (including management). Component of the Security Awareness and Training program should include Security Reminders, Protection Malicious Software, Log-in Monitoring and Password Management.	Employees are required to complete information security training upon hire and on an annual basis as a part of training compliance. Management tracks and monitors compliance with information security and awareness training requirements.
164.308 (a)(5)(ii)(A)	Security reminders: Periodic security updates.	An employee handbook is documented and reviewed on an annual basis to outline competency, evaluation, training and certification requirements.
164.308 (a)(5)(ii)(B)	Protection from malicious software: Procedures for guarding against, detecting, and reporting malicious software.	Antivirus software is installed on workstations to detect and prevent the transmission of data or files that contain certain virus signatures recognized by the antivirus software. The antivirus software provider pushes updates to the installed antivirus software as new updates/signatures are available. The antivirus software is configured to scan workstations in real time. An IPS is utilized to analyze network events and report possible or actual network security breaches.
164.308 (a)(5)(ii)(C)	Log-in monitoring: Procedures for monitoring log-in attempts and reporting discrepancies.	Monitoring software is used to identify and evaluate ongoing system performance, capacity, security threats, changing resource utilization needs and unusual system activity. The monitoring software is configured to alert IT personnel when thresholds have been exceeded.
164.308 (a)(5)(ii)(D)	Password management: Procedures for creating, changing, and safeguarding passwords.	Documented policies and procedures are in place regarding systems authentication, access, and security monitoring. Administrative access to the network is restricted to persons holding the following positions: <ul style="list-style-type: none"> • President/CEO • EVP/CSO • Director Applications Development Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include: <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(6)(i)	Security incident procedures: Implement policies and procedures to address security incidents. Policies and procedures should include response reporting.	<p>Active Directory account lockout policies are in place that include:</p> <ul style="list-style-type: none"> • Account lockout duration • Account lockout threshold • Screensaver timeout <p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>A ticket is utilized to track and respond to incidents.</p>
164.308 (a)(6)(ii)	Response and reporting: Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	<p>Documented incident response and escalation procedures for reporting security incidents are in place to guide users in identifying, reporting and mitigating failures, incidents, concerns, and other complaints.</p> <p>A ticket is utilized to track and respond to incidents.</p>
164.308 (a)(7)(i)	Contingency plan: Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain ePHI.	<p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p>
164.308 (a)(7)(ii)(A)	Data backup plan: Establish and implement procedures to create and maintain retrievable exact copies of ePHI.	<p>Data backup and restore procedures are in place to guide personnel in performing backup activities.</p> <p>An automated backup system is utilized to perform scheduled system backups.</p>
164.308 (a)(7)(ii)(B)	Disaster recovery plan: Establish (and implement as needed) procedures to restore any loss of data.	<p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p>
164.308 (a)(7)(ii)(C)	Emergency Mode Operation Plan: Establish and implement procedures to enable continuation of critical business processes for protection of the security of ePHI while operating in emergency mode.	<p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p>

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (a)(7)(ii)(D)	Testing and revision procedures: Implement procedures for periodic testing and revision of contingency plans.	A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.
164.308 (a)(7)(ii)(E)	Applications and data criticality analysis: Assess the relative criticality of specific applications and data in support of another contingency plan component.	A formal risk assessment is performed on an annual basis to identify internal and external threats and vulnerabilities that could impair system commitments and requirements. Management develops risk mitigation strategies to address risks identified during the risk assessment process.
164.308 (a)(8)	Evaluation: Perform a periodic technical and nontechnical evaluation based initially upon the standards implemented under this rule and subsequently, in response to environmental or operations changes affecting the security of ePHI, that establishes the extent to which an entity's security policies and procedures meet the requirement.	A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations. The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.
164.308 (b)(1)	Business associate contracts and other arrangements: A covered entity, in accordance with 164.306 [The Security Standards: General Rules], may permit a business associate to create, receive, maintain, or transmit ePHI on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with 164.314 [the Organization Requirements] that the business associate will appropriately safeguard the information.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(2)	A business associate may permit a business that is a subcontractor to create, receive, maintain, or transmit ePHI on its behalf only if the business associate obtains satisfactory assurances, in accordance with §164.314(a), that the subcontractor will appropriately safeguard the information.	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.308 (b)(3)	Written contract or other arrangement: Document the satisfactory assurances required by paragraph (b)(1) or (b2) above of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a) [the Organizational Requirements].	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

ADMINISTRATIVE SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.308 (b)(4)	Arrangement: Document the satisfactory assurances required by paragraph (b)(1) [the Business Associates Contracts and Other Arrangements] of this section through a written or other arrangement with the business associate that meets the applicable requirements of 164.314(a).	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.

PHYSICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.310 (a)(1)	Facility access controls: Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	This safeguard is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.
164.310 (a)(2)(i)	Contingency operations: Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	<p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p> <p>Data backup restoration test is performed on a monthly basis.</p>
164.310 (a)(2)(ii)	Facility security plan: Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	This safeguard is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.
164.310 (a)(2)(iii)	Access control and validation procedures: Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	This safeguard is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.
164.310 (a)(2)(iv)	Maintenance records: Implement policies and procedures to document repairs and modifications to the physical components of a facility which are related to security (for example, hardware, walls, doors, and locks).	This safeguard is the responsibility of the subservice organization. Refer to the "Subservice Organizations" section for controls managed by the subservice organization.
164.310 (b)	Workstation use: Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access ePHI.	Procedures that specify the proper functions, processes, and appropriate environments of workstations that access ePHI are in place.
164.310 (c)	Workstation security: Covered entities should implement physical safeguards for all workstations that access ePHI, to restrict access to authorized users.	Not applicable. The entity is not a covered entity.
164.310 (d)(1)	Device and media control: Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain ePHI into and out of a facility, and the movement of these items within the facility.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented.

PHYSICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.310 (d)(2)(i)	Disposal: Implement policies and procedures to address the final disposition of ePHI, and/or the hardware or electronic media on which it is stored.	Policy and procedure documents that address the final disposition of ePHI require that all ePHI-related media disposal be fully documented.
164.310 (d)(2)(ii)	Media re-use: Implement procedures for removal of ePHI from electronic media before the media are made available for re-use. Ensure that ePHI previously stored on electronic media cannot be accessed and reused. Identify removable media and their use. Ensure that ePHI is removed from reusable media before they are used to record new information.	Procedures for the removal of ePHI from electronic media before the media becomes made available for re-use were implemented.
164.310 (d)(2)(iii)	Accountability: Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	Procedures are in place to ensure that maintenance records of the movements of hardware and electronic media are documented. An inventory of system assets and components is maintained to record the movements of hardware and electronic media.
164.310 (d)(2)(iv)	Data backup and storage: Create a retrievable, exact copy of ePHI, when needed, before movement of equipment.	Documented backup policy and procedure documentation is in place to guide personnel in performing backups of critical ePHI. An automated backup system is utilized to perform scheduled system backups.

TECHNICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.312 (a)(1)	Access control: Implement technical policies and procedures for electronic information systems that maintain ePHI to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4) [Information Access Management].	<p>Access control and role-based build procedures are in place to restrict access to systems that maintain ePHI to only authorized personnel.</p> <p>Standardized user access request tickets are utilized to request access to ePHI prior to access being granted.</p> <p>Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity <p>Administrative access to the network is restricted to persons holding the following positions:</p> <ul style="list-style-type: none"> • President/CEO • EVP/CSO • Director Applications Development <p>Termination procedures require the removal of employee access to ePHI upon termination of employment.</p> <p>Access to ePHI is revoked as a component of the termination process.</p>
164.312 (a)(2)(i)	<p>Unique user identification: Assign a unique name and/or number for identifying and tracking user identity.</p> <p>Ensure that system activity can be traced to a specific user.</p> <p>Ensure that the necessary data is available in the system logs to support audit and other related business functions.</p>	<p>Policies are in place to guide personnel in creating, changing, and safeguarding passwords for network devices and servers.</p> <p>Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include:</p> <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity
164.312 (a)(2)(ii)	Emergency access procedure: Establish (and implement as needed) procedures for obtaining necessary ePHI during an emergency.	<p>A business continuity and disaster recovery plan are documented to identify and reduce risks, limit the consequences of damaging incidents, and ensure the timely resumption of essential operations.</p> <p>The business continuity and disaster recovery plans are developed, tested and updated on an annual basis.</p>
164.312 (a)(2)(iii)	Automatic logoff: Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	Workstations are configured to terminate inactive sessions after period of inactivity.
164.312 (a)(2)(iv)	Encryption and decryption: Implement a mechanism to encrypt and decrypt ePHI.	VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.

TECHNICAL SAFEGUARDS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.312 (b)	Audit controls: Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use ePHI.	Network devices are configured to log events and access attempts to ensure that system activity can be traced to a specific user. A ticket is utilized to track and respond to incidents.
164.312 (c)(1)	Integrity: Implement policies and procedures to protect ePHI from improper alteration or destruction.	Policies and procedures to protect ePHI from improper alteration or destruction were implemented. Administrative access to the network is restricted to persons holding the following positions: <ul style="list-style-type: none"> • President/CEO • EVP/CSO • Director Applications Development Network devices are configured to log events and access attempts to ensure that system activity can be traced to a specific user. VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (c)(2)	Mechanisms to authenticate ePHI: Implement electronic mechanisms to corroborate that ePHI has not been altered or destroyed in an unauthorized manner.	VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (d)	Person or entity authentication: Implement procedures to verify that a person or entity seeking access to ePHI is the one claimed.	Active Directory users are authenticated via individually-assigned user accounts and passwords. Active Directory is configured to enforce password requirements that include: <ul style="list-style-type: none"> • Password history • Password age (minimum & maximum) • Password length • Complexity
164.312 (e)(1)	Transmission security: Implement technical security measures to guard against unauthorized access to ePHI that is being transmitted over an electronic communications network.	VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (e)(2)(i)	Integrity controls: Implement security measures to ensure that electronically transmitted ePHI is not improperly modified without detection until disposed of.	VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.
164.312 (e)(2)(ii)	Encryption: Implement a mechanism to encrypt ePHI whenever deemed appropriate.	VPN, SSL, SFTP, and other encryption technologies are used for defined points of connectivity.

ORGANIZATIONAL REQUIREMENTS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.314 (a)(1)	Business associate contracts or other arrangements: A covered entity is not in compliance with the standards in § 164.502(e) if the covered entity knew of a pattern of an activity or practice of the business associate that constituted a material breach or violation of the business associate's obligation under the contract or other arrangement, unless the covered entity took reasonable steps to cure the breach or end the violation, as applicable, and, if such steps were unsuccessful - (A) Terminated the contract or arrangement, if feasible; or (B) If termination is not feasible, reported the problem to the Secretary."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(i)	Business Associate Contracts: A business associate contract must provide that the business associate will: "Implement safeguards that protect the confidentiality, integrity, and availability of the electronic protected health; Report to the covered entity any security incident of which it becomes aware; Authorize termination of the contract, if the covered entity determines that the business associate has violated a material term of the contract."	The entity maintains business associate agreements with businesses that create, receive maintain, or transmit ePHI.
164.314 (a)(2)(ii)	Other Arrangement: The Other Arrangements implementation specifications provide that when a covered entity and its business associate are both government entities, the covered entity may comply with the standard in either of two alternative ways: (1) if it enters into a memorandum of understanding (MOU) with the business associate and the MOU contains terms which accomplish the objectives of the Business Associate Contracts section of the Security Rule; or (2) if other law (including regulations adopted by the covered entity or its business associate) contain requirements applicable to the business associate that accomplish the objectives of the business associate contract.	Not applicable. The entity is not a government entity.
164.314 (b)(1)	Requirements for Group Health Plans: Except when the only ePHI disclosed to a plan sponsor is disclosed pursuant to §164.504(f)(1)(ii) or (iii), or as authorized under §164.508, a group health plan must ensure that its plan documents provide that the plan sponsor will reasonably and appropriately safeguard ePHI created, received, maintained, or transmitted to or by the plan sponsor on behalf of the group health plan.	Not applicable. The entity is not a plan sponsor.

ORGANIZATIONAL REQUIREMENTS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.314 (b)(2)	<p>Implementation Specifications: The plan documents of the group health plan must be amended to incorporate provisions to require the plan sponsor to-</p> <p>(i) Implement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the ePHI that it creates, receives, maintains, or transmits on behalf of the group health plan;</p> <p>(ii) Ensure that the adequate separation required by §164.504(f)(2)(iii) is supported by reasonable and appropriate security measures;</p> <p>(iii) Ensure that any agent, including a subcontractor, to whom it provides this information agrees to implement reasonable and appropriate security measures to protect the information; and</p> <p>(iv) Report to the group health plan any security incident of which it becomes aware.</p>	Not applicable. The entity is not a plan sponsor.
164.316 (a)	<p>Policies and Procedures: Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in 164.306(b)(2)(i), (ii), (iii), and (iv) [the Security Standards: General Rules, Flexibility of Approach]. This standard is not to be construed to permit or excuse an action that violates any other standard. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.</p>	The entity creates and implements appropriate policies and procedures as required by law and as suggested by good business practices and general business ethics.
164.316 (b)(1)	<p>Documentation: Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and (ii) if an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.</p>	<p>Documented policies and procedures are in place regarding systems authentication, access, and security monitoring.</p> <p>A ticket is utilized to track and respond to incidents.</p>
164.316 (b)(2)(i)	<p>Time Limit: Retain the documentation required by paragraph (b) (1) of this section for 6 years for the date of its creation or the date when it last was in effect, whichever is later.</p>	The entity retains all documentation for a minimum period of six (6) years from the date of its creation or modification, or the date when it was last in effect.

ORGANIZATIONAL REQUIREMENTS		
Ref	Regulation	Control Activity Specified by the Service Organization
164.316 (b)(2)(ii)	Availability: Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	Policy and procedures are documented for significant processes are available on the entity's intranet.
164.316 (b)(2)(iii)	Updates: Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the ePHI.	Documentation is reviewed annually and updated as needed in response to environmental or operation changes affecting the privacy or security of individually identifiable health information.

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
164.402	<p>Breach means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which compromises the security or privacy of the protected health information.</p> <p>(1)(i) For purposes of this definition, compromises the security or privacy of the protected health information means poses a significant risk of financial, reputational, or other harm to the individual.</p> <p>(ii) A use or disclosure of protected health information that does not include the identifiers listed at §164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.</p>	Breach notification procedures are in place to be used during a breach of ePHI.
164.404 (a)	<p>A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used or disclosed as a result of such breach.</p> <p>For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).</p>	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (b)	<p>Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 days after discovery of a breach.</p>	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
164.404 (c)(1)	<p>Elements of the notification required by paragraph (a) of this section shall include to the extent possible:</p> <p>(A) a brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;</p> <p>(B) a description of the types of unsecured protected health information that were involved in the breach (Such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);</p> <p>(C) any steps the individual should take to protect themselves from potential harm resulting from the breach;</p> <p>(D) a brief description of what the covered entity is doing to investigate the breach, to mitigate harm to individuals, and to protect against further breaches; and</p> <p>(E) contact procedures for individuals to ask questions or learn additional information which should include a toll-free number, an e-mail address, website, or postal address.</p>	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (c)(2)	The notification required by paragraph (a) of this section shall be written in plain language.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(i)	<p>The notification required by paragraph (a) shall be provided in the following form:</p> <p>Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be provided in one or more mailings as more information becomes available.</p>	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(1)(ii)	<p>The notification required by paragraph (a) shall be provided in the following form:</p> <p>If the covered entity knows the individual is deceased and has the address of the next of kin or personal representative of the individual (as specified under §164.502(g)(4) of subpart E) , written notification by first-class mail to either the next of kin or personal representative of the individual. The notification may be provided in one or more mailings as information is available.</p>	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
164.404 (d)(2)	Substitute notice. In the case where there is insufficient or out-of-date contact information that precludes written notification to the individual under this paragraph (d)(1)(i) of this section, a substitute form of notice reasonable calculated to reach the individual shall be provided. Substitute notice need not be provided in the case in which there is insufficient or out-of-date contact information that precludes written notification to the next of kin or personal representative of the individual under paragraph (d)(1)(ii).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(i)	In the case where there is insufficient or out-of-date contact information for fewer than 10 individuals, then substitute notice may be provided by an alternative form of written notice, telephone or other means.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(2)(ii)	In the case in which there is insufficient or out-of-date contact information for 10 or more individuals, then such substitute notice shall: (A) be in the form of either a conspicuous posting for a period of 90 days on the home page of the web site of the covered entity involved, or conspicuous notice in a major print or broadcast media in geographic areas where the individuals affected by the breach likely reside; and (B) include a toll-free number that remains active for at least 90 days where an individual can learn whether the individual's secured protected health information may be included in the breach.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.404 (d)(3)	In any case deemed by the covered entity to require urgency because of possible imminent misuse of unsecured protected health information, the covered entity may provide information to individuals by telephone or other means, as appropriate, in addition to notice provided under paragraph (d)(1) of this section.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.406	§164.406(a) For a breach of unsecured protected health information involving more than 500 residents of a State or jurisdiction, a covered entity shall, following the discovery of the breach, notify prominent media outlets serving the State or jurisdiction. (b) Except as provided in §164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach. (c) The content of the notification required by paragraph (a) shall meet the requirements of §164.404(c).	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
164.408 (a)	A covered entity shall, following the discovery of a breach of unsecured protected health information as provided in §164.404(a)(2), notify the Secretary.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (b)	For breaches of unsecured protected health information involving 500 or more individuals, a covered entity shall, except as provided in §164.412, provide the notification required by paragraph (a) contemporaneously with the notice required by §164.404(a) and in the manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.408 (c)	For breaches of unsecured protected health information involving less than 500 individuals, a covered entity shall maintain a log or other documentation of such breaches and, not later than 60 days after the end of each calendar year, provide the notification required by paragraph (a) of this section for breaches occurring during the preceding calendar year, in a manner specified on the HHS web site.	Not applicable. The entity is a business associate; its responsibilities for breach notification are limited to its covered entity customers.
164.410 (a)(1)	A business associate shall, following the discovery of a breach of unsecured protected health information, notify the covered entity of such breach.	Breach notification procedures are in place to be used during a breach of ePHI.
164.410 (a)(2)	(2) For the purposes of paragraph (1) of this section, a breach shall be treated as discovered by a business associate as of the first day on which such breach is known to the business associate or, by exercising reasonable diligence, would have been known to the business associate. A business associate shall be deemed to have knowledge of a breach if the breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person committing the breach, who is an employee, officer, or other agent of the business associate (determined in accordance with the federal common law of agency).	Policies and procedures are in place for notifying affected parties in the event of a breach of unsecured protected health information.
164.410 (b)	Except as provided in §164.412, a business associate shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after the discovery of a breach.	Documented policies and procedures are in place to guide personnel upon discovery of a breach no later than 60 days following the discovery.
164.410 (c)(1)	The notification required by paragraph (a) of this section shall include, to the extent possible, the identification of each individual whose unsecured protected health information has been or is reasonably believed by the business associate to have been accessed, acquired, used or disclosure during the breach.	Documented policies and procedures are in place to guide personnel upon discovery of a breach no later than 60 days following the discovery.

BREACH NOTIFICATION		
Ref	Regulation	Control Activity Specified by the Service Organization
164.410 (c)(2)	A business associate shall provide the covered entity with any other information that the covered entity is required to include in the notification to the individual under §164.404(c) at the time of the notification required by paragraph (a) of this section or promptly thereafter as information becomes available.	Management provides the covered entity with any information that the covered entity is required to include in the notification to the individual at the time of the breach and as soon as it is available.
164.412	If a law enforcement official states to a covered entity or business associate that a notification, notice or posting required under this subpart would impede a criminal investigation or cause damage to national security, a covered entity or business associate shall: (a) If the statement is in writing and specifies the time for which a delay is required, delay such notification, notice, or posting for the time period specified by the official; or (b) If the statement is made orally, document the statement, including the identity of the official making the statement, and delay the notification, notice, or posting temporarily and no longer than 30 days from the date of the oral statement, unless a written statement as described in paragraph (a) of this section is submitted during that time.	Documented policies and procedures are in place in the process of delaying and documenting notifications based on a law enforcement official's request.
164.414	<p>Administrative requirements and burden of proof:</p> <p>(a) covered entity is required to comply with the administrative requirements of § 164.530(b), (d), (e), (g), (h), (i), and (j) with respect to the requirements of this subpart.</p> <p>(b) In the event of a use or disclosure in violation of subpart E, the covered entity or business associate; as applicable, shall have the burden of demonstrating that all notifications were made as required by this subpart or that the use or disclosures did not constitute a breach as defined at §164.402.</p> <p>See §164.530 for definition of breach.</p>	Policies and procedures are in place for notifying affected parties in the event of a breach of unsecured protected health information.

SECTION 4

INFORMATION PROVIDED BY THE SERVICE AUDITOR

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

A-LIGN ASSURANCE's examination of the controls of CCC was limited to the Trust Services Criteria and HIPAA/HITECH requirements, related criteria and control activities specified by the management of CCC and did not encompass all aspects of CCC's operations or operations at user entities. Our examination was performed in accordance with American Institute of Certified Public Accountants (AICPA) AT-C 105 and AT-C 205.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the user auditor's objectives, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the applicable trust services criteria;
- Understand the aspects of the service organization's controls that may affect the HIPAA/HITECH requirements;
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization;
- Understand the flow of ePHI through the service organization;
- Determine whether the criteria are relevant to the user entity's assertions;
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the applicable trust services criteria; and
- Determine whether the service organization's controls are suitably designed to meet the health information security program of the user entity's and determine whether they have been implemented.

ASUS EXHIBIT H

Cyber Incident Response Policy

AUDIT SERVICES CYBER INCIDENT RESPONSE PLAN

PREPARATION

- *Ensure employees are properly trained regarding their incident response duties and responsibilities in the event of a data breach.*
- *Develop incident response drill scenarios and regularly conduct mock data breaches to evaluate our incident response plan.*
- *Ensure all aspects of ASUS incident response plan are approved and funded in advance.*

IDENTIFICATION

- *When did the event happen?*
- *How was it discovered?*
- *Who discovered it?*
- *Have any other areas been impacted?*
- *What is the scope of the compromise?*
- *Does it affect operations?*
- *Does it affect ASUS client States?*
- *Has the source of the event been discovered?*

CONTAINMENT

- *Contain the breach so it doesn't spread and cause further damage or destruction.*
- *If possible, disconnect all affected devices from the Internet.*
- *Implement short-term and long-term containment strategies.*
- *Review system and remote access protocols, change all user and administrative access credentials and change all passwords.*

ERADICATION

- *Find and eliminate the root cause of the breach.*
- *Remove all malware and verify all patches and updates have been applied.*
- *Perform thorough examination for any trace of malware or security issues remaining on system.*

RECOVERY

- *Restore and return affected systems and devices back into our business environment.*

REVIEW

- *Analyze and document everything about the breach.*
- *Determine what worked well in our response plan and more importantly, what did not work well.*

ASUS EXHIBIT I

Contract
States

ASUS Contract States and Length of Contracts

<p>Arkansas Auditor of State-21 Years Josh Wood (501) 371-2103 1400 W 3rd Street, #100 Little Rock, AR 72201-1811</p>	<p>Idaho State Tax Commission-19 Ingrid Bolen (208) 332-2978 PO Box 83720 Boise, ID 83720-9101</p>
<p>Arizona Department of Revenue-17 Will Nagel (602) 716-6033 1600 W. Monroe Phoenix, AZ 85007-2612</p>	<p>Illinois Dept. of State Treasurer-20 Roxanna Hollenstine (217) 557-4319 400 W. Monroe St., Suite 401 Springfield, IL 62704-1800</p>
<p>Controller of the State of California-14.5 Lisa Hughes (916) 322-8489 10600 White Rock Road, Ste 141 Rancho Cordova, CA 95670</p>	<p>Indiana Office of Attorney General-7 Amy Hendrix (317) 883-4521 P.O. Box 2504 Greenwood, IN 46142</p>
<p>Colorado Department of Treasury-17 Garth Farrend (303) 866-6043 1580 Logan St., Ste. 500 Denver, CO 80203-1941</p>	<p>Iowa Office of State Treasurer-18.5 Dustin McNulty (515) 725-4110 State Capitol Building Des Moines, IA 50319-0005</p>
<p>Connecticut Office of State Treasurer-15.5 John Lopes (860) 702-3276 55 Elm Street Hartford, CT 06106-1748</p>	<p>Kansas State Treasury-5 Monte Weathers (785) 291-3174 900 SW Jackson, Suite 201 Topeka, KS 66612</p>
<p>District of Columbia-6 Lynn Hall (202) 442-8193 1101 4th Street, SW, Suite W 800-B Washington, DC 20024</p>	<p>Kentucky Treasury Department-21.5 Jocky C. Denguessi Kwin (502) 564-8860 1050 US Hwy 127 South, Suite 100 Frankfort, KY 40601-2800</p>
<p>Florida Dept of Financial Services-19 Walter Graham (850) 413-5560 200 East Gaines Street Tallahassee, FL 32399</p>	<p>Louisiana Department of Treasury-21.5 Kathleen Lobell (225) 219-9377 1051 North 3rd Street, Room 150 Baton Rouge, LA 70802</p>
<p>Georgia Department of Revenue-21 James Jarrett (404) 724-7060 4125 Welcome All Road SW Atlanta, GA 30349-1824</p>	<p>Maryland Comptroller's Office-22 Maheshwar Seegopaul (410) 767-1812 301 W. Preston Street, Room 310 Baltimore, MD 21201-2383</p>

<p>Maine Office of the State Treasurer-20.5 Laura Hudson (207) 624-7466 39 State House Station Augusta, ME 04333</p>	<p>New Hampshire Treasury Dept.-18 Thomas McAnespie, Esq. (603) 271-1499 25 Capitol Street, Room 205 Concord, NH 03301-6312</p>
<p>Massachusetts State Treasurer-14.5 Mark Bracken (617) 367-0400 1 Ashburton Place, 12th Floor Boston, MA 02108-1518</p>	<p>New Jersey Dept of the Treasury-19 Steven Harris (609) 777-4655 50 Barrack Street, 6th Floor Trenton, NJ 08695-0214</p>
<p>Michigan Department of Treasury-14.5 Terry Stanton (517) 636-5313 PO Box 30756 Lansing, MI 48909-8256</p>	<p>NM Taxation & Revenue Dept-7.5 Stephanie Dennis (505) 827-0762 PO Box 25123 Santa Fe, NM 87504</p>
<p>Minnesota Dept of Commerce-20 Scott Halvorson (651) 539-1579 85 7th Place East, Suite 500 St. Paul, MN 55101-2198</p>	<p>New York Office of State Comp-11.5 Lawrence Schantz (518) 473-6318 110 State Street, 8th Floor Albany, NY 12207-2027</p>
<p>Missouri State Treasurer's Office-21 Scott Harper (573) 751-2082 P.O. Box 1272 Jefferson City, MO 65102-1272</p>	<p>North Carolina Treasury-20.5 Allen Martin (919) 814-4208 3200 Atlantic Avenue Raleigh, NC 27604</p>
<p>Montana Department of Revenue-21 Jason R. Lay (406) 444-1940 PO Box 5805 Helena, MT 59604-5805</p>	<p>ND State Land Department-20.5 Susan Dollinger (701) 328-1944 PO Box 5523 Bismarck, ND 58506-5523</p>
<p>Nebraska State Treasurer's Office-19 Megan Aguirre (402) 471-1089 809 P Street Lincoln, NE 68508-1390</p>	<p>Ohio Department of Commerce-23.5 Akil Hardy (614) 644-6094 77 S. High Street, 20th Floor Columbus, OH 43226-0545</p>
<p>Nevada Dept of Business & Industry-20.5 Linda Tobin (702) 486-4354 555 E. Washington Ave, Ste. 4200 Las Vegas, NV 89101-1070</p>	<p>Oklahoma Dept of State Treasurer-20.5 Kathy Janes (405) 522-6743 2300 N. Lincoln Blvd. Room 217 Oklahoma City, OK 73105-4801</p>

<p>Oregon Department of State Lands Claudia Ciobanu (503) 986-5248 775 Summer St. NE, Suite 100 Salem, OR 97301-1279</p> <p>Pennsylvania State Treasury Brian Munley (717) 787-3344 PO Box 1837 Harrisburg, PA 17105-1837</p> <p>RI Office of the General Treasurer Carol Aquasvivas (401) 462-7639 PO Box 1435 Providence, RI 02901-1435</p> <p>SD Office of State Treasurer Lee DeJabet (605) 773-3900 500 E. Capitol Ave Pierre, SD 57501-5007</p> <p>Tennessee Treasury Department John Gabriel (615) 253-5354 Andrew Jackson Bldg. 9th Floor Nashville, TN 37243-0203</p> <p>TX Comptroller of Public Accounts Joani Bishop (512) 463-4673 LBJ State Office Building 111 East 17 th Street Austin, TX 78774-0001</p> <p>Utah State Treasurer's Office Dennis Johnston (801) 715-3321 341 S. Main Street, 5th Floor Salt Lake City, UT 84111-2707</p>	<p>Vermont State Treasury Albert LaPerle (802) 828-1452 109 State Street, 4th Floor Montpelier, VT 05609-6200</p> <p>Virginia Department of the Treasury Bradley Earl (804) 786-3127 P.O. Box 2478 Richmond, VA 23207-2478</p> <p>Washington Dept of Revenue Barbie Proffitt (360) 534-1480 P.O. Box 34053 Olympia, WA 98504-1053</p> <p>WV Office of State Treasurer Kristi Pritt (304) 341-5047 One Player's Club Drive Charleston, WV 25311-1639</p> <p>Wisconsin Dept. of State Treasurer Amber Herman (608) 266-2390 PO Box 8982 Madison, WI 53708-8982</p> <p>Wyoming State Treasury Jeff Robertson (307) 777-5592 2020 Carey Avenue, 3rd Floor Cheyenne, WY 82002</p>
--	--

ASUS EXHIBIT J

Employee
Resumes

J. Matthew Thornton

PRINCIPAL / DIRECTOR OF OPERATIONS AUDIT SERVICES, U.S., L.L.C.

QUALIFICATIONS PROFILE

An accomplished Project Manager, Senior Consultant and Operations Manager in the Finance industry with an excellent track record of delivering the strategies and leadership that result in on-time, on-budget project fulfillment. Prior Project Management Professional (PMP) certification with an MBA in Strategic Planning.

- ♦ Able to oversee and manage all phases of the project lifecycle, from initiation to close-out.
- ♦ Skilled in unifying diverse, cross-functional teams to increase performance and achieve goals.
- ♦ Exceptional leadership and coaching skills, with a hands-on, participative management style.
- ♦ Excellent presenter, communicator, problem solver, negotiator and consensus builder.

Areas of Expertise:

- | | | |
|--------------------------------|------------------------------|---------------------------------|
| ♦ Project Planning & Execution | ♦ Team Building & Leadership | ♦ Strategic Planning |
| ♦ Business Process Design | ♦ Coaching & Mentoring | ♦ Financial Planning & Analysis |
| ♦ Technology Solutions | ♦ Client Needs Fulfillment | ♦ Operations Management |
| ♦ New Program Deployment | ♦ Contract Administration | ♦ Strategic Partnerships |

PROFESSIONAL EXPERIENCE

AUDIT SERVICES U.S., L.L.C. Principal / Director of Operations

2004 – Present

Managing member of Audit Services, U.S., L.L.C. responsible for day to day operations including data conversion, generation of all state reports and invoices, quality management and improvement efforts and the management of Audit Services' trust accounts. Also responsible for all systems development and testing projects and ensuring Audit Services' systems are in compliance with state reporting requirements.

ACS – UPRR, INC. Vice President

2002 – 2004

Responsible for the due diligence and escheatment programs for both the MetLife and John Hancock Demutualizations. Under these programs more than \$2.5 Billion was either returned to owners or escheated to various states. Also responsible for the Maximum Ownership Return program that targeted the return of property to high value shareholders for ACS-UPRR's corporate actions customers.

MELLON INVESTOR SERVICES, L.L.C. Vice President

1997 – 2002

Senior Operating Executive credited with pioneering use of Project Management principles throughout organization with 1,500 employees and \$250 million in annual revenues, with frequent lead role in multimillion-dollar, high-profile projects that transcended product lines and departments. Coordinated client, vendor, and organizational activities to facilitate on-time, on-budget project fulfillment. Forged strategic alliances with key domestic and international financial institutions.

...Continued...

AMERICAN MANAGEMENT SYSTEMS, INC.**1995 – 1997****Business Systems Consultant / Project Manager**

Consulted with client companies to provide expertise and feasible solutions for broad range of technology projects and disciplines. Visited clients on-site to build strong relationships, assess clients' needs, coordinate activities, and direct team members; reported project status to client and employer. Successfully employed project management methodologies to meet client requirements.

FIRST NATIONAL BANK OF CHICAGO**1989 – 1995****Product Manager (1994 – 1995); Strategic Planning Analyst (1993);
Manager, Financial Planning & Analysis (1989 – 1992)**

Built distinguished record of achievement and advancement through increasingly responsible positions. Scope of responsibility encompassed project management, staff training and development, financial planning and analysis, internal consulting, strategic planning, product management, business development, and general management functions.

EDUCATION & CREDENTIALS

MBA in Management/Strategic Planning – Fordham University Graduate School of Business

BBA in Finance – University of Massachusetts at Amherst

Project Management Professional (PMP) Certification – Project Management Institute (through 2005)

Jeremy D. Katz

Key Accomplishments

- 25 years of unclaimed property experience
- Led team that developed patented unclaimed property auditing process
- Managed MissingMoney.com for over 14 years
- Worked with all 50 states' unclaimed property programs
- Successfully facilitated the recovery of hundreds of millions of dollars to the states' unclaimed property programs

Experience

Audit Services US, LLC, Partner, New York, NY (Dec. 2016 - Present)

Joined firm as Partner to lead significant expansion of existing unclaimed property compliance service offerings, as well as to develop new solutions involving advanced compliance analytics. Transitioned unclaimed property practice established at PRA to Audit Services.

PRA Government Services, LLC, Vice President, State Government Solutions, White Plains, NY (Sep. 2014 - Nov. 2016)

Created and implemented a state government focused sales and marketing program designed to leverage PRA's core competencies in unclaimed property, tax/revenue auditing, discovery, collections and revenue administration.

Xerox (formerly Affiliated Computer Services, Inc. (ACS)) State Government Enterprise Solutions Group, White Plains, NY (Jan. 1995 - Sep. 2014) (Included Unclaimed Property Clearinghouse and State Business Process Solutions)

Chief Operating Officer, Xerox State Business Process Solutions (January 2012 - September 2014)

Direct all aspects of business development, program implementation, ongoing operational and relationship management, and have P&L accountability for \$60 million plus line business. Lead operational management team responsible for 300 individuals to ensure that all quarterly and annual financial, growth and operational objectives are accomplished. Drive growth and profit objectives through the acquisition of new business, as well as maximize growth opportunities within existing accounts, review business processes to ensure that profit is maximized and to maintain or exceed required and expected service levels, and serve as the executive interface with government agency leadership. Initiate and manage all lobbying activities, media relations, consulting/partnership/teaming arrangements and trade organization participation.

Develop budgets, forecasts, financial models, reports and conduct management presentations to senior executive leadership.

Vice President, Government Business Development and Sales (May 2003 - January 2012)

Managed national government relations initiatives, sales and new product development in State Treasurer, Comptroller, Finance, Tax and Revenue marketplace. Key accomplishments included the implementation of a formalized account management and sales program, the launch of highly successful compliance and revenue solution and the re-launch and enhancement of an existing web-based eligibility solution (MissingMoney.com). These initiatives resulted in a contract renewal rate of greater than 95% and increased market penetration in two key services areas by more than 25%. Total contract value for renewals and new business was several hundred million dollars.

Responsible for creating a formalized sales program and managed a team responsible for selling services relating to: revenue enhancement and discovery, statutory compliance/audit, web-based customer support applications, securities custody, claims processing and call center/customer care programs. Sales efforts have focused on business process outsource and information technology-related solutions, including: finance and tax applications, cloud-based computing, infrastructure management, enterprise print management and application development and maintenance.

Other responsibilities included: serving as high-level client relationship manager and advising on all matters relating to sales initiatives, proposal development, contract negotiations and client problem resolution. Directed national lobbyist, consultant and community outreach activities in support of sales and legislative objectives.

Vice President of State Government Relations (Jan. 1998 to May 2003)

Served as relationship manager with state program administrators, treasurers, and other government officials. Communicated services and initiatives to state officials in order to identify client business needs and grow existing accounts to full potential. Secured and negotiated contracts with client states. Managed media relations program and served as spokesperson on behalf of company to print, radio and television media. Monitored industry-related legislation and coordinated all lobbying efforts. Wrote content for newsletters, trade journals and other communications materials. During this time period and the time period listed below as Director of Marketing, market penetration increased from 30 to 50 states and revenue doubled. Total contract value was in the tens of millions.

Director of Marketing (Jan. 1995 - Jan. 1997)

Wrote and implemented company's marketing and communications plan. Created service literature, public information pieces and sales presentations. Developed and managed a proprietary sales database to improve and measure the effectiveness of marketing initiatives, create revenue forecasts and rank prospects. Maintained active relationships with members of press and trade associations. Issued frequent press releases and

communications pieces to national, regional and trade publications, resulting in appearances in hundreds of publications, generating thousands of sales leads.

The Onyx Group, Alexandria, VA, Business Manager (Jan. 1994 - Jan. 1995)

Contract administrator and liaison with all federal and state government clients. Developed and maintained system for collecting data used for billing projections, staffing requirements and project management. Managed project group to develop and market multi-media information system for regional business development organization.

***United States Treasury Department, Internal Revenue Service,
Headquarters Office of Strategic Business Planning***

Washington, DC Planning Analyst (May 1991 - Jan. 1994)

Worked with analysts and functional representatives to develop IRS' strategic business plan. Compiled and analyzed data related to strategic management process. Wrote sections of business review reports used by IRS' senior executives. Performed research and analysis for development of performance measurement system. Developed statements of work for management consulting contracts and served as a Contracting Officer Technical Representative.

Education

University of Maryland, College Park, Maryland, BA, August 1990

Major: Government and Politics Minor: English

Johns Hopkins University, Baltimore, Maryland, Graduate course work in Marketing Management, International Marketing, Public Relations and Information Systems Planning.

Board Memberships

- Served 3 year term on the National Association of State Treasurer's Corporate Affiliate's Board.
- Served two 2 year terms on National Association of State Treasurer's Foundation Board.
- Served as lead faculty advisor for National Institute of Public Finance Treasury Management Program.

Awards

- ACS/Xerox Team Excellence Award - 2005
- ACS/Xerox Leadership Excellence Award - 2006
- ACS/Xerox President's Club Award - 2007
- ACS/Xerox President's Club Award - 2009

Benjamin C. Spann

Talented Management professional with exceptional Computer and Communication Skills

- Over 30 years of Unclaimed Property experience.
- Familiar with UPS2000, UPMS and HRS software.
- Consistent record of increased collections/refunds.
- Knowledgeable in all aspects of Unclaimed Property.
- Former NAUPA Regional Vice President.
- Self motivated team player/builder.
- Excellent presentation/communication skills.
- Recipient of Multiple NAUPA awards.

PROFESSIONAL EXPERIENCE

Audit Services, U.S., LLC, New York, NY
Chief Executive Officer

2013 - Present

Louisiana Department of the Treasury, Baton Rouge, LA
Director of Unclaimed Property

2000 – 2012

- Increased collections from \$21 million to \$60 million per year.
- Increased refunds from \$8 million to \$25 million per year.
- Involved in the implementation of a digital imaging system.
- Testified at Louisiana Legislative Committee hearings.
- Responsible for \$2 million dollar annual budget.
- Responsible for audit reviews and audit selections.
- .

Louisiana Department of Revenue, Baton Rouge, LA
Director of Unclaimed Property

1986 – 2000

- Authored Louisiana's first comprehensive Unclaimed Property law revision.
- Organized and implemented the Unclaimed Property Division.
- Increased collections from \$3 million to \$21 million per year.
- Increased refunds from \$290,000 to \$8 million per year.
- Served as sole I/T Division support for UPMS software.
- Developed and operated the NAUPA bulletin board system prior to the internet.
- Developed and operated the first NAUPA website.

Louisiana Department of Revenue, Baton Rouge, LA
Auditor

1976 – 1986

- Field Audit Assignment Control and Audit Selection.
- Developed the Department's first computerized audit tracking system.
 - Performed Louisiana Oil & Gas Severance Tax audits
 - Performed Louisiana Income and Corporation Franchise Tax audits
 - Performed Louisiana General Sales Tax audits

**Cycle Specialties, Ruston, LA
Sales & Parts Specialist**

1974 – 1975

- Sold new & used motorcycles
- Sold new parts for motorcycles

EDUCATION*BS in Accounting*, Louisiana Tech University, Ruston, LA (1975)**COMPUTER SKILLS**

Windows Operating Systems (98/NT/2000/XP), Linux, OS/2, Word, Excel, Access, Crystal Report Writer, FoxPro, PowerPoint, Publisher, Pro-1099, web design and SQL

LICENSES

FAA private aircraft pilot license (not current)

AWARDS AND HONORS

2008 NAUPA Lifetime Achievement Award
NAUPA President's Distinguished Service Award
NAUPA Appreciation Award

ADDITIONAL INFORMATION

Database Administrator for Broadmoor High School Class of 1971 reunion committee.
Webmaster for a non-profit car club.
Volunteer at St. James Episcopal Church.
Panelist at numerous NAUPA conferences.
Testified before numerous Louisiana Legislative committee hearings.
Louisiana Treasury representative speaking at numerous conferences, radio shows, television shows and public appearances.

Amy Manganaro

AUDIT MANAGER



PROFESSIONAL PROFILE

I am a hard-working and dedicated employee with a passion for working with unclaimed property. I work very well with others in a team setting but work equally as well independently. I consider the ideal job to be one that challenges me every day and one where I am constantly learning, evolving, and bettering myself as an employee.

SKILLS

Attention to Detail
Time Management
Dependability
Team Leadership
Project Planning
Accountability
Improving Efficiency
Customer Service
Creativity
Resource Management
Computer Skills

EDUCATION

MASTER'S DEGREE

Business Administration
Trevecca Nazarene University
Nashville, TN
2005 – 2007

BACHELOR OF ARTS

Business Administration
Concentration: Accounting
Minor: French
Eastern Nazarene College
Quincy, MA
1995 – 1999

VOLUNTEER

Ruff Tales Rescue (MA)
2018-current

EXPERIENCE

AUDIT MANAGER

Audit Services U.S., LLC/January 2017-Current

Lead unclaimed property examinations on behalf of state clients in order to ensure compliance with state regulations.

- Prepare and maintain document requests submitted to holders for audits.
- Analyze documentation received from holders related to all general ledger activity in order to prepare audit workbooks.
- Communicate with holders, holder advocates, and holder counsel on regular basis related to audit status and documentation.
- Work in a team setting to provide coverage and support for other ASUS Audit Managers.
- Manage all aspects of approximately 15 examinations at a given time.
- Utilize interactive audit tracking system to provide audit status and pertinent audit information to fellow team members.

LEAD EXAMINER

PRA Government Services/January 2016-January 2017

Conduct audits of holders in multiple industries and establish procedures and protocols for unclaimed property audit department.

- Establish audit requests, training materials, policies and procedures for department.
- Participate in weekly status calls providing management with updates on examinations.
- Assist team members with Contractor-Assisted Self Audits (CASA)
- Lead examinations of holders and participate in all aspects of the audit from Opening Conferences to workbook preparation and remediation review.
- Attend National Association of State Treasurers (NAST) conference in New Orleans, LA.

AUDIT SUPERVISOR

Xerox/January 2015-January 2016

SENIOR AUDITOR

Xerox/June 2012-January 2015

Lead unclaimed property audits on behalf of state clients. Manage audit staff on projects in order to move audits toward conclusion in a timely and effective manner while producing thorough results for our clients.

- Provide management with pertinent data analysis in order to perform scoping exercises on potential audit candidates.
- Maintain 25+ active audits at any given time either independently or with assigned staff to examinations.
- Lead examination of holders of many types of industries with areas of audit focus in general ledger activity, rebates and life insurance.
- Participate in opening conferences and regular status calls with holders.
- Provide updates to clients on a monthly basis regarding status of examinations.
- Draft detailed audit reports of processes performed and present them to holders and/or state clients.
- Train new staff members on processes and procedures.

UNCLAIMED PROPERTY MANAGER ACCOUNTING SUPERVISOR

Optum Insight (f/k/a AIM Healthcare)/August 2002-June 2012

Responsible for all escheatment processes related to three holders. Additionally, responsible for two full-time employees and one contractor related to accounting responsibilities while working remotely from home.

- Prepare escheatment accounting entries, reconciliation of accounts, due diligence letters, and state reports for three holders.
- Attend Unclaimed Property Professionals Organization (UPPO) annual conferences.
- Lead accounting processes related to two lines of business including daily reconciliations and month-end close processes.
- Manage full-time employees and maintain all associated tasks including annual performance reviews and evaluations.



Erik J. Kallevik

OBJECTIVE

To seek an Unclaimed Property management position that would capitalize on my professional auditing and accounting skills, interpersonal skills and educational background.

COMPUTER SKILLS

- MS Excel, Word, PowerPoint, Access, Outlook, SharePoint, ZOHO, Visual Basic, Oracle Essbase Financial System, SAP, PeopleSoft, Oracle, Apprise, Great Plains, QuickBooks & Adobe Acrobat Professional

PROFESSIONAL EXPERIENCE

Audit Services U.S., LLC, New York, NY 2017-Present **Audit Manager**

- Manage several billion-dollar corporate audits performing all phases of Unclaimed Property examinations; targeting potential holders, scope analysis, risk assessment, fieldwork, review State Statutes and collect Unclaimed Property findings for authorized states.
- Analyze essential aspects of Financial Reports (corporate tax returns, GL trial balances, bank records, etc.) to identify the potential unclaimed property.
- Communicate with holders and holder advocates to ensure deadlines are met and act as a liaison between the holder and the state Unclaimed Property Administrators.
- Maintain an open line of communication with senior management on the progress of examinations while requesting feedback on the proper direction to mitigate risk.

Kelmar Associates, LLC, Wakefield, MA 2014-2017 **Audit Manager**

- Manage a team of Associates and Senior Associates to effectively complete Unclaimed Property examinations (15+ audits) in accordance with defined procedures and documentation standards.
- Communicate with holders and holder advocates to ensure deadlines are met and act as a liaison between the holder and the state Unclaimed Property Administrators.
- Challenge and inspire Associates and Senior Associates to achieve a high level of productivity in their work while maintaining high morale.
- Maintain an open line of communication with senior management on the progress of examinations while requesting feedback on the proper direction to mitigate risk.
- Analyze essential aspects of Financial Reports (corporate tax returns, GL trial balances, bank records, etc.) to identify the potential unclaimed property.

Xerox State & Local Solutions / Unclaimed Property Clearinghouse, Quincy, MA 2010-2014 **Audit Manager (2012-2014) & Senior Auditor (2010-2012)**

- Managed several multi-billion dollar corporate audits performing all phases of Unclaimed Property examinations; targeting potential holders, scope analysis, risk assessment, fieldwork, consult General Counsel and collect Unclaimed Property findings for authorized states.
- Supervised / delegated projects to auditors to progress all Unclaimed Property audits. Audit analysis performed for all General Ledger account types, which include Accounts Payable, Accounts Receivable, Payroll, Unidentified Receipts and industry specific property types.

- Work in conjunction with VP of Audit and C-level executives to accurately budget and forecast revenue and audit timelines.
- Communicate with holders, holder advocates and state Unclaimed Property Administrators to ensure deadlines are met and act as a liaison between the holder and the state.
- Performed multiple training seminars at Xerox's multi-state Unclaimed Property conferences to educate state administrators in Unclaimed Property auditing skills and new trends in the industry.

Forrester Research, Cambridge, MA

2009-2010

Senior Accountant

- Performed a management role by supervising the Travel & Entertainment (T&E) team to ensure employees are abiding by Forrester's T&E policy.
- Service support leader for the Forrester's PeopleSoft employee help-desk, guided employees on the PeopleSoft expense process and resolved any troubleshoot questions that may arise.
- Supervise Accounts Payable process to ensure vendors are paid accurately and in a timely manner.
- Produced, analyzed and presented Financial Reports to both the Controller and Chief Accounting Officer: Accounts Payable, Expense Accruals, Domestic and International Bank Reconciliation, Income Statement Analysis and any other ad hoc reports that were requested on a monthly basis.
- Assisted in implementing a new T&E process to enforce Forrester's T&E policy, saving the company thousands of dollars per week.

First Act, Incorporated, Boston, MA

2007-2009

Accounting/Finance Manager

- Produced many of the Financial Reports for First Act: Accounts Receivable, Accounts Payable, Inventory, Prepaid and Accrual, Depreciation, Bank Reconciliation and Cash Flow.
- Prepared tax reporting documents (sales tax, corporate tax and 1099 reporting).
- Supervised the Accounts Payable department, to ensure vendors were paid on a timely basis.
- Coordinated with departments to provide a monthly financial review and create the annual budget.
- Worked with auditors to mitigate risk within the accounting and finance departments.
- Streamlined the monthly reporting process by 20% through automating excel reports and cutting repetitive processes through organization and communication among team.

KPMG International, Boston, MA

2005-2007

Senior Associate - Internal Audit & Regulatory Compliance

- Supported corporate internal controls by mitigating risk and abiding by government regulations while satisfying organizational goals and objectives.
- Analyzed business processes to identify high risk controls, audit planning, development of audit programs, and testing of internal controls of critical business areas (such as finance, billing, accounting, external reporting (10K, 10Q), investment management, Sarbanes Oxley 404 compliance, marketing, HR, etc...) for companies in the Financial Services, Commercial Banking, Wealth Management, Consumer Goods, Telecommunications & Equipment Rental industries.
- Evaluated results of test work, developed recommendations to mitigate residual risks and/or improve efficiency of the operation, and delivered recommendations to management.

State Street Corporation, Boston, MA

2004-2005

Assistant Controller

- Assisted the Senior Money Market Controller, within the Global Treasury division, by creating the financial reports for State Street Corporation.
- Created, analyzed and audited the Money Market's daily, monthly and quarterly reports which were distributed to various Directors, Vice Presidents and Executive Vice Presidents within State Street Global Markets and Global Treasury divisions.
- Streamlined financial reports by using Excel macros and formulas, which increased the accuracy of the reports while cutting the labor hours to create the Executive Committee financial reports by a third.
- Maintained the general ledger and worked with Sarbanes-Oxley Section 404 compliance, forecasting, budgeting and verifying invoices.

Auditor

2002-2004

- Auditing our client, General Electric Asset Management's accounts (custody and non-custody portfolios), to verify the integrity of their monthly financial records.

- Researched and reconciled exceptions: outstanding receivables and payables, failed trades, past due income, pending foreign exchanges and share discrepancies.
- Worked closely with the Quality Assurance team and IT department to communicate any issues identified and correct the financial portfolios.

Senior Portfolio Accountant
Portfolio Accountant

1999-2002
1998-1999

EDUCATION

B.S., Resource Economics with a concentration in Managerial Accounting
University of Massachusetts, Amherst, MA 1998

James C. Dowley



**Examiner Training & Management - Customer Service – Negotiator –
Managerial Reporting – Management of Outside Contractors– Experienced Presentation Speaker**

Uniquely positioned to deliver unclaimed property compliance examination results with extensive experience developing and implementing solutions combined with wide-ranging knowledge of state's unclaimed property laws.

Unclaimed Property Examination Administrator

Long term experience administering unclaimed property examination programs. Consistent record of success leading teams of unclaimed property examiners to deliver high quality work product which complies with professional standards and state laws. Broad vision and perspective with focus on maximizing the number of examinations completed annually and unclaimed monies collected.

PROFESSIONAL EXPERIENCE

Unclaimed Property Auditor; Audit Services, U.S., LLC

July 5, 2017 to Present

- Plan, determine scope and perform unclaimed property compliance examinations of large public & private corporations which comply with professional standards and state unclaimed property laws.
- Analyze documentation, prepare examination working papers, present findings and analyze remediation to determine total unclaimed property reporting liability.
- Work with internal and external company representatives to facilitate the examination process.
- Update managerial reports tracking examination progress.

Director of Audits, Conduent State & Local Solutions, Inc.

June 26, 2016 to June 23, 2017

- Coordinate audit work of a team of seven professional auditors relating to unclaimed property examinations of large national companies to insure compliance with professional standards and state unclaimed property laws.
- Analyze reports from audit managers and compile detailed examination status reports for management.
- Maintain and update monthly Work-In-Process reports for state clients.
- Communicate with state clients and companies under audit to address issues and facilitate the audit process.
- Management duties include conducting period performance reviews; ongoing counsel and participation in the hiring and termination process.

Compliance Supervisor, Ohio Division of Unclaimed Funds, Columbus, Ohio

September 1998 to October 2015

- Administered the State of Ohio's internal field and desk examination functions.
- Developed and documented examination procedures, techniques and methods.
- Determined the scope, planned and scheduled field examinations, reviewed and approved working paper files, negotiated settlements and collected unclaimed funds due.
- Responsible for training and developing field and desk examination personnel.

- Maintained extensive examination statistics to provide detailed reports of the results of examination programs to management.
- Managed orientation and training program for the State's field & desk examiners and contractors.
- Oversaw the and facilitated the State's contract examination programs
 - Monitored the contract examination process to insure compliance with Ohio Administrative Code rules.
 - Developed relationships with contractors.
- Supervised internal and external customer service and support of Ohio Business Gateway, HRS Pro software and UP Exchange application
- Functioned as division spokesperson at seminars who proficiently delivered presentations to professional groups of CPAs, attorneys and other business professionals.

ACCOMPLISHMENTS

- Designed and implemented a Professionals Education Program (PEP) targeting professional groups in the state such as Certified Public Accountants (CPAs), attorneys, trust agents and payroll managers to educate them about the State's unclaimed funds reporting requirements.
- Collaborated with Division counsel to write administrative rules for Ohio's unclaimed funds field examinations for State personnel and outside contractors.
- Developed Agreed-Upon Procedures for use by Certified Public Accountant contractors performing in-state examinations according to Ohio Administrative Rules.
- Successfully reinitiated the State's in-house unclaimed funds examination program by hiring, training and completing field examinations with a new staff of four (4) field examiners in two (2) months.

Unclaimed Funds Auditor 4

Ohio Department of Commerce, Division of Unclaimed Funds 1988 to 1998

- Planned, determined scope and performed unclaimed funds examinations of large companies including financial institutions, public & private corporations, trust companies and utility companies
- Made recommendations to company representatives regarding internal control and data processing changes needed to comply with the Ohio Unclaimed Funds Law.
- Prepared working papers and reports for company representative and managerial reporting.

EDUCATIONAL BACKGROUND

Bachelor of Science, Business Finance, The Ohio State University, Columbus, OH, 1982

TECHNICAL EXPERTISE

Microsoft Access, Excel, Word & Outlook, Crystal Reports, UPS2000, HRS Pro and UP Exchange

William W. Joseph Jr.

Education

9/5/00 – Present	William Paterson University Major: Computer Science	Wayne, NJ
10/13/97 – 3/11/99	Computer Learning Center, Inc Associate's Degree: Computer Programming	Paramus, NJ

Career Experience

7/7/04 – Present	Audit Services U.S., LLC Reports Processing Manager <ul style="list-style-type: none"> • Convert various input formats into NAUPA reporting format • Verify and correct supplied data to conform with NAUPA regulations • Generate State specific reports, coverletters, and forms • Create, verify and supply data diskettes containing NAUPA reports for each state • Troubleshoot and assist auditors and state employees with reporting questions and issues • Assist in ongoing development of company specific software • Verify holder information for claims 	New York, NY
0/9/03 – 7/6/04	Oltron, Inc: X-Ray and Digital Imaging Webmaster/Field Service Technician <ul style="list-style-type: none"> • Created and maintained corporate website using JavaScript and HTML • Repaired and refurbished X-Ray equipment throughout the New York metropolitan area • Integrated computer technology in the installation and calibration of X-Ray generators • Sustained verbal and written communications with clientele 	Carlstadt, NJ
9/27/01 – 9/7/03	Consultant Private Consultant <ul style="list-style-type: none"> • Composed customer database system to aid in the organization of Insurance company clients • Designed a parts/equipment inventory program using Visual Basic and Microsoft Access for an X-Ray imaging company • Employed artistic talents in the development and maintenance of web sites for online gaming communities • Constructed interactive portfolio software to highlight client's proficiency as an educator 	Wayne, NJ

7/6/98 – 9/26/01	<p>Dunlop, Onderdonk & Wilson Corp. / Bollinger, Inc. Short Hills, NJ</p> <p>Network Administrator / Information Systems Technician</p> <ul style="list-style-type: none"> • Administered and maintained Windows NT network • Isolated computer system failures to the component level • Diagnosed and repaired workstations and HP Laserjet printers • Initiated reorganization of software and hardware components • Assisted Help Desk with hardware and software concerns • Supplied technical support to colleagues in operating system transition from DOS to Windows 98/2k platforms • Educated personnel in the use of the agency management software, as well as, the Internet and Microsoft Outlook
------------------	---

Computer Literacy

Programming Languages: Visual Basic, SQL, HTML, XML, XHTML, DHTML, Java, J++.
 JavaScript, Visual C++, COBOL, JCL, CICS, FoxPro, and PHP

Software Packages:	<p>Windows (3.1-XP), MS Office (95 – 2k), Ebix.One AMS, Adobe Photoshop, Illustrator, Macromedia Flash, Microsoft Developer Studio, CorelDraw, Dreamweaver, 3D Studio Max, Frontpage, Poser, DAZStudio</p>
--------------------	--

Organization Membership:	<p>Ebix.One Community, Microsoft Developer Network Member</p>
--------------------------	---

VIRGILIO CAPALA JR.



EDUCATION

The Chubb Institute, Jersey City, New Jersey Diploma in Computer Programming	1996
University of San Carlos, Cebu City, Philippines Completed 120 units toward BSECE (Bachelor of Science in Electronics and Communication Engineering)	1990

TECHNICAL SUMMARY

HARDWARE: IBM 3090, IBM Compatible PC

SOFTWARE:

Mainframe: COBOL, COBOL II, MVS/ESA, MVS/JCL, VSAM, IDCAMS, CICS,
DB2, OS UTILITIES, TSO/ISPF-PDF, EZTRIEVE
PC: Microsoft Office

CONCEPTS: Problem Analysis, Basic and Advanced Programming Design and Techniques in
Online and Batch Processing, Dumps Debugging and Management Utilities, File updating
and Manipulation (VSAM, Physical Sequential and DB2), System Maintenance

EXPERIENCE

Audit Services US, LLC, New York, New York Escheatment Systems Analyst	2013-Present
Computershare, Jersey City, New Jersey Escheat Securities Analyst	2012- 2013
BNY Mellon Shareowner Services, Jersey City, New Jersey (Acquired by Computershare January/2012) Escheat Securities Analyst	2012-2012
BNY Mellon Shareowner Services, Jersey City, New Jersey (Merger of BNY and Mellon in July/2007) Escheat Securities Analyst	2007-2012
Mellon Shareowner Services, Ridgefield Park, New Jersey Escheat Securities Analyst	2004-2007

- In house consultant of Escheat system
- Identify system bugs and request system modifications
- Created a process using Eztrieve to identify escheatable accounts not pickup by the Mainframe program .(This was used to identify system gap)
- Created a system using Access database to identify escheatable CUSIPs using the various data pull from various reports/system
- Reformat reports into a one line data to import in excel for analysis

Mellon Shareholder Services, Ridgefield Park, New Jersey 2000-2004
(Acquired Chasemellon in Dec/2000)

Programmer

- Created a check payment system for Tobacco Settlement project.
- Part of the team that converted the check database from VSAM based to DB2
- Created an online application to view checks and create various check transactions
- Supports nightly batch process

Chasemellon Shareholder Services, Ridgefield Park, New Jersey 1997-2000

Programmer

- Y2K remediation – Expand the 6 digit to 8 digit date on the batch and online jobs
- Tested and debugged programs after file expansion

ARGI, Montvale, New Jersey 1996-1997

Programmer

- Convert name and address data from various layout into one standard format to create mail records

Margola Corporation, New York, New York 1991-1996

System Application Maintenance

- Maintain an accounting software (MAS90) with 16 users including one online user in NY-NJ office
- Trouble shoot, analyze & fix systems and terminal hang-up
- Write and generate customized reports using the Report Master (4GL software included in MAS90 program)
- Set-up password for individual user
- Set-up new forms for printing such as checks, sales order, invoices and shipping label
- Perform monthly and yearly period processing
- Write system modifications to programmer to modify the program to fit company needs

Radio Shack, New York, New York 1990-1991

Salesperson

- Certified Computer Sales Specialist
- Help customers solve computer related problems

Jeffrey L. Saitta



Software Developer

Education:

SUNNY at Farmingdale, NY
Computer Sciences

Hardware:

IBM S/3, 34, 36, 38, AS/400

Software Languages:

RPG/ III, IV, ILE, QRY, SQL

Business Experience:

Audit Services

212 W 35rd Street
New York, NY 10001

Dates: 5/2004 to present

Duties: Utilizing my 26 years of programming experience to develop and maintain all software used by ASUS's staff.

Working closely with staff designing new projects as well as maintaining and the improvement of existing systems.

Conversion of data received by transfer agent and formatted to the AS/400.

Tracking System

Due Diligence

Property Eligibility

Event Date Analysis

NAUPA State Filing

Reconciliation/Scheduling

Dividend Processing

Work In Process Analysis

Reporting and Inquiry Systems

Jeffrey L. Saitta



Unclaimed Property Recovery and Reporting

450 7th Avenue
New York, NY 10001

Dates: 1/1999 to 5/2004

Duties: Programmed major Recovery system to return unclaimed property to shareholder's before escheating those funds to appropriate states. Responsible for all new and existing programming needs for an Escheatment system.

Scotti Financial Data Services

163Varick Street
New York, NY 10013

Dates: 2/1996 to 1/1999

Hired as consultant by CHASEMELLON Bank to redesign there Corporate Reorganization System. Programs developed enabled staff to process a shareholder claim from 13 days to 3. Daily duties included converting data files from transfer agent, debiting and crediting of stocks, printing checks and stock certificates.

ACS Financial Securities & Services

915 Broadway
New York, NY 10010

Dates: 9/1983 – 2/1996

Duties: Debiting/Crediting of publicly traded stocks and bonds.

David Potter (Legal Support)

David Potter is an accomplished litigator, having conducted over 35 jury trials, 100 bench trials and hearings, and numerous appellate arguments in state and federal courts. For over 25 years, he served as a faculty member for the National Institute of Trial Advocacy and Hofstra University Trial Techniques Program. Mr. Potter has also been a frequent commentator on Court TV.

Mr. Potter began his legal career as a New York City Assistant District Attorney, where he initially handled drug, larceny and corruption cases. Less than three years after joining the District Attorney's office, he was promoted to the position of trial attorney in the Homicide Bureau. Mr. Potter later joined a 60-lawyer business law firm in New York and transitioned into civil litigation.

In 1993, Mr. Potter co-founded the law firm of Lazare Potter & Giacobas (now Lazare Potter Giacobas & Moyle), where he continued representing clients in a wide range of commercial matters. He currently represents clients in complex commercial litigations, arbitrations and mediations, contract negotiations and employment matters.

Education

- Albany Law School of Union University, Albany, New York (J.D., 1986 - Recipient, Order of the Barristers Award)
- St. Lawrence University, Canton, New York (B.A., 1982)

Bar Admissions

- States of New York and Massachusetts • District of Columbia
- U.S. Court of Appeals for the Second Circuit
- U.S. District Courts for the Southern and Eastern Districts of New York

James Moyle (Legal Support)

Mr. Moyle's practice covers a broad range of industries and includes commercial litigation, arbitrations, regulatory investigations, securities class and derivative actions and employment issues. The flexibility of his practice allows Mr. Moyle to represent companies as well as individual officers, directors and employees in important matters whether large or small.

Mr. Moyle's successful track record over more than twenty-five years has earned him repeated recognition as one of New York's leading business lawyers. Chambers USA, for example, has described him as a "superb litigator" and "an excellent tactician." Some of the nation's most respected companies turn to him for a variety of matters that demand a sophisticated yet pragmatic approach. Mr. Moyle's strategic advice has resulted in many early-stage victories, and has allowed clients to manage risk and control costs by positioning cases for highly favorable settlements.

Mr. Moyle is also an experienced courtroom advocate, and in one case the winning jury verdict after a six-week trial was hailed by the National Law Journal as one of the "Top Defense Wins of the Year." He also has successfully litigated matters before administrative courts, including a recent win against the SEC's Division of Enforcement in the first case ever brought under new Regulation A+.

Before starting his own firm, Mr. Moyle was a partner at Alston & Bird LLP and at Clifford Chance LLP, one of the world's largest firms, where he was a two-term member of the firm's global governing board. Mr. Moyle has authored numerous articles on financial services litigation and is a member of the New York State Bar Association, the New York City Bar Association, and the Federal Bar Council.

Education

- Albany Law School of Union University (JD, magna cum laude, 1991)
- State University of New York at Binghamton (BA, English with honors, 1988)

Bar Admissions

- New York
- United States Supreme Court
- United States Court of Appeals for the Second Circuit
- United States Court of Appeals for the Third Circuit
- United States Court of Appeals for the Seventh Circuit
- United States District Court for the Southern District of New York
- United States District Court for the Eastern District of New York
- United States District Court for the Central District of Illinois

ASUS EXHIBIT K

Audit
Authorization
Letter

SAMPLE AUTHORIZATION/ENGAGEMENT LETTER
(State Letterhead)

[Date]

[Individuals Name]

[Title]

[Company Name]

[Address]

[City, State, Zip]

Dear Mr. (Last Name);

The [Department] of the State of (the "State"), pursuant to authority granted to it under [Statute], has scheduled an examination of your books and records for the purpose of determining compliance with the Unclaimed Property Law. The examination of [Company] will include all relevant property subject to unclaimed property reporting under [Statute], and will involve the parent company, subsidiaries, divisions and affiliates.

The examination will be conducted by Audit Services (ASUS) as our authorized agent. ASUS has been directed to analyze all unclaimed property in order to determine that portion that should be subject to the custodianship of the State. A representative of ASUS will contact you to schedule a mutually convenient date to begin the review of your records. You will be advised of the records and personnel, and possible third parties, which need to be accessible for the examination. At the conclusion of the examination, please process all reportable unclaimed property records through ASUS.

The [Department] reserves the right to impose interest, penalties and examination costs permitted under the Law for failure to report or deliver abandoned property.

If you should have any questions, please contact the ASUS Audit Manager, at (123) 456-7890 or auditmanager@auditservicesus.com.

Sincerely,

[Agency]

[Title]

ASUS EXHIBIT L

Audit
Services
System

The Audit Services System

Overview of Data Processing Environment & System Architecture

The **Audit Services System** provides the processing which produces client reports to state unclaimed property departments. Our processing software stands alone and is designed for the specific purpose of processing unclaimed property data for compliance reporting. As such we do not require interface with any other vendors or software in the course of providing our services. The **Audit Services System** is located offsite in Pearl River, New York and it operates on an IBM AS400 platform.

- **Importing Corporate Property Records**

The **Audit Services System** has a dynamic import function that allows the mapping of fields on an imported file into the system. The **Audit Services System** is compatible with data received in all standard electronic (spreadsheet or text file) formats.

We would ideally receive an electronic file of inactive/outstanding accounts and checks from each division or subsidiary entity of the Company for which we are auditing, processing and reporting, in either a MS Excel Worksheet (.xls), MS Access Database (.mdb), or ASCII Text File (.txt) format. The fields included in the data records will have been agreed upon during pre-implementation discussion. Data in hardcopy form or in nonstandard electronic formats typically requires our staff to directly enter or further convert the files before importation.

The file may be delivered to ASUS via email attachment or electronically, depending on file size and security considerations. ASUS is capable of receiving a file of any size via internet connectivity.

- **System Updates for State Compliance**

The **Audit Services System** is constantly updated to meet changing state and corporate requirements. Our AUDIT SERVICES Data Analyst tracks all state documentation of reporting deadlines, property type and dormancy period data on an ongoing basis. ASUS maintains contact with all state unclaimed property administrators and will be advised of any new data requirements. Should there be an update in mandatory data requirements or reporting deadlines from a particular state, ASUS updates the system and informs the staff when the information is made public. The time frame to comply with the new data request will vary depending on when ASUS receives the information. In the past, anticipated changes have normally been communicated by states on a timely basis.

AUDIT SERVICES Process Quality Control and Review

ASUS management is responsible for the development and maintenance of the **Audit Services System**, maintenance of the internal network, and maintenance of applications essential to data processing, including updates of the operating system and applications ensuring security of client data. The **Audit Services System** is fully protected from unauthorized access to state and corporate data residing on the system. ASUS has established a firewall between the system site servers and the Internet. Access to the ASUS local network and applications is likewise prevented by the lack of external connectivity. Security monitoring is therefore limited to monitoring internal access to the system and data. Internal access to the system and client state data is controlled and monitored by the ASUS network administrator. All data is archived separately and backed up on tape daily. Back-up tapes are stored off-site. In the event of a significant outage, system service will normally be restored within 24 hours.

All system implementation and maintenance is authorized by ASUS management and supervised by the ASUS processing administrator. In order to ensure accuracy, the **Audit Services System** is tested thoroughly whenever an upgrade or fix is implemented. System tests may include both live and fabricated data testing procedures. All testing is done in-house at ASUS. No client state or third-party interaction for testing is necessary.

Periodic internal reviews include ad hoc reporting to client states and response to inquiries by holders and states to determine the consistency of the data archived with the data submitted. Environmental controls are evaluated regularly as a function of maintenance and improvement of the system.

It is ASUS policy never to share client data with anyone outside of ASUS unless explicitly instructed to do so by the client state.

Compliance Reporting on Required Forms

The **Audit Services System** is compliant with the reporting requirements of all 50 states and 4 jurisdictions. Most states accept a common reporting format, known as the "NAUPA format", established in 1995. Most states accept reports in an electronic format, however, some states have unique reporting and remittance requirements. The **Audit Services System** automatically produces the electronic and paper-reporting formats each state requires. ASUS provides the flexibility of reporting by multiple entities or reporting by the parent for multiple entities. When ASUS submits a report by the parent for multiple entities all entities covered by the report are identified to the states.

ASUS EXHIBIT M

APEARS
Instructions



Using the Individual Lookup:

Step 1:

Using credentials provided by CCC, enter user name and password. They are case sensitive. Also the disclaimer **MUST** be clicked and the check box clicked to enter the site. This must be done for each session. A user's session will automatically end after 20 minutes of inactivity. After that, you will be required to log in again. **It's recommended that when you are done with the system, you utilize the 'Log Out' menu option located at the bottom of the left navigation menu.**



Step 2:

Currently your credentials give you access to 'Individual Lookups' as accessed by the left hand menu(not shown here). Within this lookup, you can do the following:

- Lookup by full SSN or partial SSN
- Lookup by combination of criteria([First Name], [Last Name], [State], [Birth Month], [Birth Day], [Birth Year]), along with Partial SSN.
- Automatic wildcards usage.
 - Definition: if first name and last name are entered(i.e. Anita Inkles), the search criteria will be any [First Name] **starting** with 'Anita' and [Last Name] **beginning** with 'Inkles'
 - If you turn off 'Automatic Wildcards', then the above example will look for **exact** [First Name] and [Last Name] of 'Anita' and 'Inkles'
 - However, with 'Automatic Wildcards' off, you then can customize [First Name] and [Last Name] by entering the following:
 - All [First Name] exact match to 'Anita'



- All [Last Name] beginning with 'Inkles%' ← Notice that I added the % for wildcard usage for last name.
- Results returned are limited to 25 records
 - If your criteria is too broad, you will be notified to supply additional criteria to narrow the search.
 - If the criteria does not find any hits, you will be notified that no records exist that match criteria supplied.
- When results are returned in the grid(if they are <= 25 records), clicking on the SSN will populate a new grid with additional information particular to the individual you are looking for,
 - Hovering over the [Last Residence Zip Code] in the particular record will display the city, state and zip of the last known residence of the found person(see below).

- SSN and BirthDate require the wildcard(in all cases) if partial information is entered.(see snapshot 2).
 - I entered partial information for the year(191%), but a full segment for the first 3 digits of the SSN, so SSN did not need the '%'
 - **Suggestion: I'd leave 'Automatic Wildcards Use' on for now**
- **Search Example:**
 - I want to search for any one whose SSN begins with '042' AND
 - [First Name] begins with 'ANITA' AND
 - [Last Name] begins with 'INKLES' AND
 - [State] is 'NY' AND
 - [Birth Year] is '1917'
 - See **Snapshot 3** for how this would be setup within the Lookup window:

Snapshot 1:



APEARS INDIVIDUAL LOOKUP [Help](#)

☒ Automatic Wildcards Use?

SSN:	<input type="text"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
State:	<input type="text" value="=> SELECT =>"/>
Birth MM/DD/YYYY	<input type="text"/>

Snapshot 2:

APEARS INDIVIDUAL LOOKUP [Help](#)

☒ Automatic Wildcards Use?

SSN:	<input type="text" value="[REDACTED]"/>
First Name	<input type="text"/>
Last Name	<input type="text"/>
State:	<input type="text" value="NY"/>
Birth MM/DD/YYYY	<input type="text" value="[REDACTED]"/>

REVIEW:
This search will return: 1,165.
Display of NTIS' LADMF protected records are limited to 25 for legal and security purposes.
Please refine your search by adding criteria or removing wildcards.

SNAPSHOT 3:

APEARS INDIVIDUAL LOOKUP [Help](#)

☒ Automatic Wildcards Use?

SSN:	<input type="text" value="[REDACTED]"/>
First Name	<input type="text" value="[REDACTED]"/>
Last Name	<input type="text" value="[REDACTED]"/>
State:	<input type="text" value="[REDACTED]"/>
Birth MM/DD/YYYY	<input type="text" value="[REDACTED]"/>

REVIEW:
No Records Found for this criteria.

ASUS EXHIBIT N

Sample
Global Audit
Resolution

SAMPLE AUDIT RESOLUTION AGREEMENT

This Audit Resolution Agreement dated as of [DATE] is entered into by and among Audit Services U.S., LLC (“Auditor”), The [COMPANY NAME] (“Company”) and those States identified in the attached **Schedule A** that have executed this Agreement as provided herein (the “Participating States”). Company, Auditor and the Participating States shall collectively be referred to herein as the “Parties.”

WHEREAS, Auditor is conducting an audit of Company and its affiliates to identify property belonging to property owners that was required to be reported and remitted to the Participating States pursuant to the UP Laws (as such term is defined below);

WHEREAS, Company is cooperating with the Participating States and Auditor by making its books and records available for examination and its personnel and agents available to assist as requested by the Participating States and Auditor;

WHEREAS, Company and the Participating States recognize that a multi-state audit of this nature may be complex and time-consuming and that, in the absence of a prior understanding between the Parties, disputes may arise concerning how the audit should be conducted; and

WHEREAS, Company and the Participating States desire to avoid unnecessary disputes and to have the audit conducted in the most efficient and effective manner possible;

NOW, THEREFORE, the Parties agree as follows:

I. Definitions

For purposes of this Agreement, capitalized terms have the meanings set forth below:

(a) **“Agreement”** means this Audit Resolution Agreement entered into among the Participating States, Company, and Auditor.

(b) **“Audit”** means the unclaimed property audit that Auditor has been conducting of Company and its affiliates, on behalf of the Participating States, which is being resolved with respect to the Participating States pursuant to the Agreement.

(c) **“Dormancy Period”** means the period of years as defined in **Schedule B** of this Agreement upon the expiration of which the unclaimed property is escheatable to the Participating State.

(d) **“Interested Person”** means and includes, with respect to property: (i) a person designated in a written document maintained in the records of the Company as an authorized representative of the owner of the property with full access to the account; (ii) a court-appointed guardian or custodian of the owner; (iii) an attorney-in-fact on behalf of the owner; (iv) a court appointed estate representative, including but not limited to an administrator or executor, of a deceased owner; or (v) any other person who has, or who Company in good faith believes has a legal right to ownership or custody of the property, including for the avoidance of doubt, any named beneficiary of a deceased owner.

(e) **“Last Known Address”** means, with respect to an apparent owner of property, the address of record in the Company’s systems; provided that if there is no such address of record, or if such address of record is insufficient for the delivery of mail, any description, code, or other indication of the location of the apparent owner which identifies the state, even if the description, code, or indication of location is not sufficient to direct the delivery of first-class United States mail to the apparent owner may be used as the Last Known Address.

(1) If the United States postal zip code associated with the apparent owner is for a post office, the state in which such post office is located will be deemed to be the state of the last-

known address of the apparent owner unless other records associated with the apparent owner specifically identify the physical address of the apparent owner to be in another state.

(2) For property with a beneficiary (or beneficiaries) designated to receive the account funds on the property owner's death, the relevant Last Known Address shall be of the original property owner, even if the owner is deceased, until such time as the property has been transferred to the person (or persons) entitled to the funds in the account.

(f) **"Mailing Address"** means, with respect to an owner of property, the address used by Company to send account-related communications.

(g) **"Owner-Generated Activity"** means any verifiable communication from or activity initiated by an owner of the property or other Interested Person, as recorded in the books and records of Company, including, without limitation, depositing funds into or withdrawing funds from the account (by check, or by ACH, wire, internal, or other transfer), making electronic distributions, contacting Company by telephone, interactive voice response unit, online or mobile account ("Account Center") or otherwise to discuss or conduct account-related matters, sending Company paperwork or documents related to the account, modifying the account or owner profile, sending Company correspondence regarding the account via e-mail, the Account Center, facsimile, or other electronic means, U.S. Postal Service or other mail vendor, submitting an account service request through the Account Center, setting up the account for electronic delivery of communications, taking a distribution, and accessing the account via the Account Center or other electronic means. Recurring financial transactions or activity pursuant to a standing owner instruction, such as automatic payments, deposits, withdrawals, contributions, or distributions (collectively, "Recurring Transactions") shall not be considered Owner-Generated Activity. Owner-Generated Activity is distinguishable from activity generated solely by Company such as,

without limitation, crediting dividends or interest, posting account fees, and mailing account statements and other account related information, which does not constitute Owner-Generated Activity. Owner-Generated Activity on one account of an owner shall be considered activity on all other accounts which that owner has the power to control or in which the owner holds an interest.

(h) **“Parties”** means the Participating States, Auditor, and Company; “Party” shall mean any one of the Parties.

(i) **“Retirement Account”** means a Traditional IRA or a Roth IRA.

(i) **“RMD Date”** means April 1 following the year in which the owner reached age 70½, except that (1) if the owner attained age 70½ after December 31, 2019, RMD Date means April 1 following the year in which the owner reached age 72; and (2) if the owner attained age 70½ in 2019, RMD Date means April 1, 2021.

(j) **“Roth IRA”** means a Roth individual retirement account, as defined or described in the Internal Revenue Code of 1986, as amended, and the rules and regulations thereunder.

(k) **“Scope of the Audit”** means (i) all Retirement Accounts for which Company is the custodian with a Last Known Address in a Participating State and Accounts for which there is no Last Known Address; and (ii) all uncashed checks distributed from such Retirement Accounts, if the amount represented by the uncashed check is still owed to the owner of the check or the owner’s beneficiary if the owner is deceased.

(l) **“Traditional IRA”** means a traditional individual retirement account, as defined or described in the Internal Revenue Code of 1986, as amended, and the rules and regulations thereunder.

(m) **“Unclaimed Property Report” or “UPR”** means a report prepared and submitted to Company by Auditor identifying property that Auditor has determined to be escheatable under the Agreement.

(n) **“UP Laws”** means the unclaimed property/escheat laws of the Participating States, as applicable.

II. Effective Date

The Agreement shall not become effective until executed by Company, the Auditor, STATE NAME and at least two other States. The “Effective Date” of the Agreement shall be the latest of (a) the date upon which Auditor provides notice to all Parties that the Agreement has been executed by STATE NAME and two of the other States listed on **Schedule A** and delivers the executed Agreement copies to Company; (b) the date upon which Auditor delivers the Executed Agreement copy to Company; and (c) the date upon which Company delivers the Agreement Executed Agreement copy to Auditor; provided, however, that if a State executes the Agreement after the later of such dates, then the Effective Date as to that State only shall be the date on which Auditor has delivered the executed copy of the Agreement by such State to Company. In accordance with the foregoing but for the avoidance of any doubt, not all States listed in **Schedule A** shall be required to execute the Agreement in order for it to be effective as to the Participating States that do execute it. Notwithstanding the foregoing, if a State does not execute the Agreement within ninety (90) days after the date the Agreement is executed by Company, the Agreement shall not be effective as to such State (and such State shall not be considered a Participating State for purposes of this Agreement) unless the Company agrees in writing that the Agreement shall be effective as to such State.

III. Standards for Escheatment

The parties agree that the escheatment standards with respect to the Participating States for purposes of this Audit are set forth below.

A. Retirement Accounts

Property in a Retirement Account subject to the Scope of the Audit is escheatable if there has been no Owner-Generated Activity regarding the account during the Dormancy Period, which begins on the respective date described in clauses 1 and 2 below, and continues for the applicable period set forth on **Schedule B**.

1. **Traditional IRAs.** The Dormancy Period for a Traditional IRA begins on the following dates:
 - a. If the account owner is alive, the latest of (i) the RMD Date; (ii) the date of the last Owner-Generated Activity; or (iii) when one or more pieces of mail have been returned to the Company as undeliverable or the Company has discontinued mailings to the owner.
 - b. If the account owner died on or after January 1, 2020 and the beneficiary is an “eligible designated beneficiary” or “non-eligible designated beneficiary,” as such terms are used in the Setting Every Community Up for Retirement Enhancement (SECURE) Act of 2019, Pub. L. 116–94 (the “SECURE Act”), the later of (i) the last day of the tenth year following the year in which the owner’s death occurred; and (ii) the date of the last Owner-Generated Activity; provided, however, that if the sole beneficiary is the spouse of the owner, then the spouse shall be deemed to be the owner of the account and the Dormancy Period shall not begin until the conditions set forth in this Section III(A)(1) are met with respect to the spouse.

- c. If the account owner died prior to January 1, 2020 and on or after the RMD Date, or the account owner died on or after January 1, 2020 and on or after the RMD Date and the beneficiary is neither an “eligible designated beneficiary” or “non-eligible designated beneficiary,” as such terms are used in the SECURE Act, the later of (i) the last day of the year following the year in which the owner’s death occurred, and (ii) the date of the last Owner-Generated Activity; provided, however, that if a beneficiary is the spouse of the owner, then the spouse shall be deemed to be the owner of the account and the Dormancy Period shall not begin until the conditions set forth in this Section III(A)(1) are met with respect to the spouse.
 - d. If the account owner died prior to January 1, 2020 and before the RMD Date, or the account owner died on or after January 1, 2020 and before the RMD Date and the beneficiary is neither an “eligible designated beneficiary” or “non-eligible designated beneficiary,” as such terms are used in the SECURE Act, the later of (i) the last day of the fifth year following the year in which the owner’s death occurred); provided that the year 2020 is not counted for purposes of calculating this five-year period, and (ii) the date of the last Owner-Generated Activity.
2. **Roth IRAs.** The Dormancy Period for a Roth IRA begins on the later of (i) the last day of the fifth year (or tenth year, if the owner died on or after January 1, 2020 and the beneficiary is an “eligible designated beneficiary” or “non-eligible designated beneficiary,” as such terms are used in the SECURE Act) following the year in which the owner’s death occurred; provided that the year 2020 is not

counted for purposes of calculating this five-year period; and (ii) the date of the last Owner-Generated Activity; provided, however, that if the sole beneficiary is the spouse of the owner, then the spouse shall be considered the owner of the account and the Dormancy Period shall not begin until the conditions set forth in this Section III(A)(2) are met with respect to the spouse as owner.

3. If Company's records do not reflect the owner's date of birth for a Retirement Account (or if the date of birth appears clearly erroneous), such date of birth shall be presumed, for purposes of determining the RMD Date, to be 21 years before the date the account was opened, provided however, if the date of birth of the spouse deemed to be the owner under Section III(A)(1) or III(A)(2) is not reflected in Company's records (or if the date of birth is clearly erroneous), no such presumption shall apply to such spouse and the account will be deemed to have been opened on the date opened by the original owner.
4. An account owner is presumed dead if the records of the Company provide that the owner is deceased.
5. The Auditor shall have the opportunity to run the names of the IRA account owners through the United States Social Security Administration Death Master File ("Death Master File") as part of its audit. Any disputes regarding whether an account owner's appearance on the Death Master File is reliable evidence of the owner's death shall, for purposes of determining the commencement of the Dormancy Period, be resolved pursuant to Section VI hereof.

6. For purposes of this Section III, the “owner” of the account means the original accountholder until such time as the accountholder has been confirmed to be deceased and the property in the account has been transferred to a beneficiary.

B. Uncashed Checks

At the time any Retirement Account is escheatable under this Section, any unclaimed interest, dividend, or increment associated with the property (a “Distribution”) will also be escheatable. If property in a Retirement Account is not yet escheatable under the standards set forth above, Distributions paid in the form of a check from a Retirement Account to the owner are escheatable if the check payable to the owner remains outstanding and there has been no other Owner-Generated Activity regarding the Distribution during the Dormancy Period as set forth on **Schedule B**. With respect to any such Distribution, the Dormancy Period begins on the date the Distribution was made.

C. Change in Law

If there is a change in law (including as the result of a precedential court ruling for a Participating State) that materially modifies the escheatment standards as set forth above with application to property covered by the Audit prior to the date property is required to be escheated to a Participating State hereunder, the Parties will attempt in good faith to agree upon any necessary revision to the appropriate standards to be applied. If the Parties cannot agree to a modification, then the standard set forth above shall remain applicable with respect to Company’s obligation to produce information required hereunder; however, Company and the Participating State shall each have the right to rely on the change in the law with respect to any dispute over whether property is subject to escheatment.

Furthermore, if any Participating State issues any administrative guidance, pronouncement or other public statement (“Guidance”) prior to the date property is required to be escheated to the Participating State hereunder which, if applied to any property within the Scope of the Audit, would mean that such property is not required to be escheated, then Company may rely on such Guidance to not escheat the property to the Participating State pursuant to this Agreement, provided that the Company identifies the Guidance being relied upon and the property not being escheated as a result of that Guidance. No such Guidance will affect the Company’s obligations to provide information required hereunder. In case of ambiguity regarding whether such Guidance does not require property to be escheated to a Participating State, the Participating State will determine whether such Guidance means the Company is not required to escheat the property.

IV. Submission of Data and Unclaimed Property Report

Auditor and the Participating States acknowledge and agree that (a) Company has previously provided data on property within the Scope of the Audit; and (b) Auditor has previously determined that (1) 417 Traditional IRAs with Last Known Addresses in the Participating States may potentially be presumed abandoned and escheatable to such States; and (2) 58 Roth IRAs with Last Known Addresses in the Participating States (such Traditional IRAs and Roth IRAs, the “Review Population”) may potentially be presumed abandoned and escheatable to such State. Company and Auditor will work cooperatively and in good faith to determine, based on the application of the standards described herein, whether any of such property in the Review Population is required to be escheated to a Participating State.

Within ninety (90) days of the Effective Date, Auditor will submit a revised unclaimed property report to Company identifying all property within the Scope of the Audit which Auditor

has determined is escheatable under the terms of this Agreement (the “UPR”). The UPR will be delivered in the format of the “Submission Workbook” that Auditor previously sent to Company.

Following receipt of the UPR, Company shall have ninety (90) days to review the property listed on the UPR in order to identify all property that it agrees is escheatable under the terms of this Agreement as well as any exceptions it may have to the property reviewed (the “Review Period”). On or prior to the expiration of the Review Period, Company shall provide Auditor with a list identifying all reviewed property it agrees is escheatable under the Agreement (subject to due diligence as described below), as well as any property that Company has determined is not escheatable under the Agreement, together with the specific reasons for its exceptions. Where the grounds for the exceptions are based on documents or data that have not been previously provided to Auditor, Company shall include such data or documentation. Auditor may request additional data from Company with respect to any properties for which Company takes an exception; provided, however, that Company shall not be required to provide or otherwise disclose any information to Auditor or any Participating State if such disclosure would violate any privacy laws or any other laws, rules, or regulations applicable to Company, provided that the Company identifies the law, rule or regulation that would allegedly be violated, nor shall Company be required to provide Auditor with access to its facilities or systems. In the event the Company withholds any information from the auditor based on the foregoing sentence, the Participating States will have the right to issue a subpoena for the information or commence a proceeding to obtain the information, which the Company may oppose.

Auditor expressly acknowledges that the Nondisclosure Agreement (“NDA”) previously entered into between Auditor and Company shall apply to all information and data provided by Company under this Agreement, and that Auditor shall continue to be bound by the NDA. For the

avoidance of doubt, this Agreement shall not amend or supersede any provision of the NDA. In the event of a conflict between the terms of this Agreement and the terms of the NDA, the terms of the NDA shall govern.

E. Data Processing Issues

Auditor shall give notice to Company of any data provided by Company that Auditor is unable to reasonably process. Company shall use reasonable efforts to provide the data in a format that Auditor is reasonably able to process. Auditor agrees that it is able to accept data provided in Microsoft Excel spreadsheets.

V. Exceptions to Property Listed on Unclaimed Property Report

Company shall be entitled to dispute the escheatability of property listed on the UPR based on any one or more of the following grounds (“exceptions”):

1. The standards for determining that property is escheatable under the Agreement have not been met;
2. There has been a verifiable communication from or confirmed contact with the owner or any Interested Person after commencement of the Dormancy Period;
3. The property is not within the Scope of the Audit;
4. The property was required to be reported to a Participating State more than ten (10) years prior to the Effective Date (based on the standards as set forth in this Agreement), except that (a) for Texas, the period of time shall be seven (7) years; (b) for North Dakota, the period of time shall be five (5) years; and (c) for Idaho, the period of time shall be three (3) years; or
5. Company and Auditor and/or any Participating State agree that the property should not be deemed abandoned and reportable for any reason.

VI. Resolving Disputes Regarding Unclaimed Property Report or Other Matters

If Company identifies any exceptions to the UPR, Auditor shall have forty-five (45) days to review the exceptions. If it disputes any exceptions, it shall notify Company in writing of the disputed exception(s) and describe the reason for the dispute. Auditor agrees that it may only dispute an exception if the property is escheatable based on the standards set forth in this Agreement (as may be amended based on any change in law or administrative guidance as described in Section III). If Auditor disputes any exceptions on behalf of a Participating State, then Auditor and Company and, if necessary, such Participating State, shall meet in good faith to resolve the dispute within twenty (20) days following notice thereof. If Company, Auditor and the Participating State are unable to resolve any exception within sixty (60) days after Company and Auditor first meet to discuss the exception, the dispute shall be resolved pursuant to mandatory arbitration (other than to the extent prohibited by applicable law with respect to a Participating State) as described below. The existence of an unresolved dispute as to reporting and remitting of certain property shall not affect the duty to report and remit property as to which no dispute exists. All unresolved disputed exceptions involving all Participating States shall be arbitrated by the Parties together in one arbitration proceeding, except to the extent a Participating State is prohibited by law from participating.

Any other disputes regarding this Agreement shall also be resolved pursuant to mandatory arbitration, as described below, except with respect to a Participating State that is prohibited by law from submitting to such arbitration.

(a) **Governing Law and Rules.** This arbitration provision is governed by the Federal Arbitration Act (“FAA”). Arbitration must proceed only with the American Arbitration Association (“AAA”) or JAMS. The rules for the arbitration will be those in this arbitration

agreement and the procedures of the chosen arbitration organization, but the rules in this arbitration agreement will be followed if there is disagreement between the agreement and the organization's procedures. If the organization's procedures change after the claim is filed, the procedures in effect when the claim was filed will apply. If both AAA and JAMS are unavailable, and if the Parties cannot agree on a substitute, then either Auditor or Company may request that a court appoint a substitute.

(b) Fees and Costs. Each Party will bear its own fees and costs in connection with the arbitration.

(c) Hearings and Decisions. Arbitration hearings will take place in the federal judicial district for the Eastern District of Pennsylvania unless otherwise agreed by the parties. A single arbitrator will be appointed. The arbitrator must:

- Follow the terms of this Agreement;
- Follow all applicable substantive law, except when contradicted by the FAA or superseded by the terms of this Agreement;
- Follow applicable statutes of limitations;
- Honor valid claims of privilege; and
- Issue a written decision including the reasons for the award.

(d) Arbitrator Decision and Appeal. The arbitrator's decision will be final and binding except for any review allowed by the FAA. However, if more than \$100,000 was genuinely in dispute for a single Participating State or \$500,000 was genuinely in dispute for all Participating States, then either Party may choose to appeal to a new panel of three arbitrators. The appellate panel is completely free to accept or reject the entire original award or any part of it. The appeal must be filed with the arbitration organization not later than 30 days after the original award issues.

The appealing party pays all appellate costs unless the appellate panel determines otherwise as part of its award. Any arbitration award may be enforced (such as through a judgment) in any court with jurisdiction.

VII. Due Diligence

Company shall perform due diligence on property that is escheatable under the Agreement prior to remittance to a Participating State. Company shall complete the due diligence within ninety (90) days following the end of the Review Period (the “Due Diligence Deadline”); provided, however, that for any property that an arbitrator has determined is escheatable pursuant to Section VI, the Due Diligence Deadline shall be ninety (90) days following the arbitrator’s decision.

Company’s due diligence pursuant to this Section VII shall include the following:

1. If Company’s records do not indicate the Last Known Address of an owner is incorrect (*i.e.*, mail has been sent to the owner and has been returned as undeliverable on two consecutive occasions), Company shall mail at least one letter to the owner at the Last Known Address reminding the owner that s/he has property in the custody of Company and informing the owner that such property will be escheated if the owner does not make contact with Company. For property with a deceased owner, Company shall send the due diligence letter to the estate representative or other Interested Persons, if known to Company.

2. If an account has a Mailing Address and Company’s records do not indicate that it is incorrect, Company shall mail at least one letter to the owner at the Mailing Address reminding the owner that s/he has property in the custody of Company and informing the owner that such property will be escheated if the owner does not make contact with Company. The letter shall comply with the language requirements of the UP Laws; provided, however, that the letter shall

be deemed to have satisfied the requirements of the UP Laws if it is substantially in the form attached as Exhibit 1 hereto.

Company may also elect, but is not required, to conduct any additional due diligence by the Due Diligence Deadline that Company believes would be helpful to locate or make contact with the owner or any Interested Person with respect to the property.

If Company, based on information it has obtained through its due diligence efforts, has a good faith belief that additional time will allow Company to make contact with the owner or other Interested Person, and notifies Auditor of such belief, the Due Diligence Deadline shall be extended by sixty (60) days.

Within thirty (30) business days following the end of the Due Diligence Deadline, Company shall provide Auditor with a list of all owners or other Interested Persons with whom it has made documented contact as a result of the due diligence process, and all property for which due diligence has been completed and that is to be remitted to a Participating State.

VIII. Remittance of Property

A. State of Remittance

Property shall be remitted to the state of the Last Known Address of the owner of the property solely to the extent that such state is a Participating State. Property shall not be reported and remitted under the Agreement unless the Last Known Address of the owner of the property is in a Participating State.

B. Timing and Coordination of Remittance

Within sixty (60) days after the Due Diligence Deadline, Company shall remit the property determined to be escheatable to the relevant States and which has not been returned to the owners or other Interested Persons or determined not to be owed pursuant to the due diligence process.

All property subject to this Agreement (other than property reported by Company to any Participating State in the ordinary course of business) shall be remitted by Company to each Participating State either through Auditor or in accordance with Auditor's reasonable instructions and shall be reported by Company to Participating States with a notation indicating that the report is made pursuant to the Audit. Company shall provide Auditor with a copy of all such reports and remittances.

C. Waiver of Penalties and Interest

The Participating States agree to waive any and all penalties and interest on any property that has been or will be escheated in connection with the Audit, provided that Company materially complies with all provisions of this Agreement.

IX. General Provisions

(a) In the event that a Participating State materially breaches this Agreement, Company shall have the right to terminate this Agreement with respect to such Participating State and any property related thereto. In the event that the Auditor materially breaches this Agreement, Company shall have the right to terminate this Agreement in its entirety. In the event that Company breaches this Agreement as to any Participating State, such Participating State may terminate this Agreement as to itself. Notwithstanding the foregoing, a Party shall not be entitled to terminate this Agreement for material breach unless such material breach has continued after the Party alleging breach has provided the alleged breaching Party with detailed written notice of the breach and an opportunity to cure such breach for twenty (20) days. The Parties agree that a breach of this Agreement by any Party may cause another Party irreparable damage, and therefore the non-breaching Party shall be entitled to specific performance and injunctive relief as a remedy for any such breach from any court of competent jurisdiction. The right to seek and obtain specific

performance and injunctive relief shall not limit such Party's right to pursue other remedies. All remedies available to any Party for breach of this Agreement by another Party are and shall be deemed cumulative and may be exercised separately or concurrently.

(b) In the event of a breach or claimed breach or termination of this Agreement by Company as to one or more Participating State(s), such breach or claimed breach or termination shall not constitute a claimed breach or breach or termination of the Agreement, or affect the enforceability of this Agreement, as between Company and the other unaffected Participating State(s). In the event of a breach or claimed breach of this Agreement by one or more Participating State(s), and Company has terminated the Participating State(s) from this Agreement in accordance with Subsection IX(a), such termination shall not constitute a termination of the Agreement, or affect the enforceability of this Agreement, as between Company and the other non-terminated Participating State(s).

(c) Upon written request, Company agrees to provide reasonable assistance to a Participating State to aid the Participating State in determining the validity of claims made upon property remitted under the Agreement.

(d) Each Participating State agrees that if, hereafter, another person, entity, or state makes any claim with respect to any of the property remitted under this Agreement by Company, the applicable Participating State, upon written notice of such claim, will hold harmless and indemnify Company against any and all liability, costs, fees, and damages with respect to such claim, to the extent permitted by law. Such Participating State shall also, at its own expense, defend Company against any such claims, if Company so requests. Any person claiming an interest in his, her or its unclaimed property paid under this Agreement may also file a claim thereto under the provisions of the applicable Participating State's UP Laws.

(e) Upon Company making all reports and remittances required under the Agreement to a Participating State, either directly or through the Auditor, the Participating State hereby agrees that Company shall be released from all claims, demands, interest, penalties, actions, liabilities, or causes of action that the Participating State may have as of that date regarding, arising out of, or relating to any property within the Scope of the Audit (a “Release”); provided that, accounts that are not escheatable as of the Effective Date, but may become escheatable after the Effective Date, shall not be property within the Scope of the Audit. At such time, the audit of Company by such Participating State shall be deemed concluded. Company shall be deemed to have made all reports and remittances required under this Agreement if Company has reported and remitted all property agreed to be escheatable by both Company and Auditor, or determined to be escheatable by an arbitrator pursuant to the dispute resolution provisions of Section VI. Any immaterial failure to make a report or remittance as to particular property shall not affect a Release. Furthermore, if Auditor identifies any errors with any reports or remittances made under this Agreement, Auditor shall promptly notify Company of same, and Company shall have a reasonable period of time not less than thirty (30) days to correct such errors. The Release provided in this Section shall apply if Company corrects any errors identified by Auditor. Auditor shall have no more than ninety (90) days after submission of each report and remittance to identify any errors to Company.

(f) Auditor and the Participating States agree to maintain the confidentiality of information disclosed by Company including, without limitation, information concerning the business processes and trade secrets of Company to the extent permissible under each Participating State’s laws, and shall only disclose such information to the extent required under each Participating State’s laws.

(g) Neither the Agreement, nor any act performed or document executed in furtherance of the Agreement, nor any discussions or communications leading to the Agreement, is now or may be deemed in the future to be an admission or evidence of liability or wrongdoing by Company or any of its current or former affiliates, subsidiaries, officers, directors, employees, agents, or representatives. In addition, nothing in this Agreement shall be construed to imply that the Company was or is required by any law or regulation to escheat any property based on the dormancy standards set forth in Section III, nor shall such dormancy standards establish any precedent or obligation for the Company to escheat any property in the future based on the same or similar dormancy standards.

(h) The Auditor and the Participating States acknowledge that Company is entering into this Agreement in a voluntary and cooperative attempt to comply with the Participating States' UP Laws. Accordingly, the Auditor and the Participating States agree not to make comments or statements in connection with the execution of this Agreement that criticize, condemn, or minimize the competence, integrity, quality, or reputation of Company, nor shall the Auditor or any Participating State make any comment or statement suggesting that the execution of this Agreement by Company establishes or suggests Company's non-compliance with any law. The Company agrees that it shall not criticize, condemn, or minimize the competence, integrity, quality, or reputation of the Auditor or the Participating States.

(i) Each Party shall be excused from its performance under the Agreement, shall not be deemed to have breached the Agreement, and shall not be liable in damages or otherwise in the event of any delay or default in performance under the Agreement resulting from a circumstance that is either (i) not within the reasonable control of such Party including, but not limited to, damage to or destruction of such Party's or its agents' property, systems, or facilities; or (ii) caused

by another Party. Notwithstanding such circumstances, each Party shall exercise reasonable diligence to perform its obligations under the Agreement and shall take reasonable precautions to avoid the effects of such circumstances to the extent that they may cause delay or default with respect to such Party's ability to perform its obligations under the Agreement.

(j) The Agreement and its Schedules constitute the entire agreement of the Parties with respect to the matters referenced herein and may not be amended or modified, nor may any of its terms be waived, except by an amendment or other written document signed by the Parties thereto; provided however, that a Participating State and the Company may agree to amend or modify this Agreement with respect to such Participating State without the signature of the other Participating States.

(k) The Agreement shall not confer any rights upon any person or entity other than the Parties and is not intended to be used for any other purpose. Nothing in the Agreement shall be construed to provide for a private right of action to any person or entity, nor shall the Agreement be deemed to create any intended or incidental third-party beneficiaries.

(l) Each Party represents and warrants that the individual signing the Agreement on its behalf has authority to do so.

(m) The Agreement may be executed in counterparts, but shall not be effective except as provided for in Section II above.

(n) Either Company or Auditor may request a reasonable extension for any deadline set forth in this Agreement, and the other party shall not unreasonably withhold its approval of any such request as long as the other party has been acting in good faith in connection with the examination.

(o) This Agreement will be governed by, and construed in accordance with, the internal laws of the Commonwealth of Pennsylvania, without regard to its choice of laws principles; provided however, that the UP Laws of each Participating State shall apply over Pennsylvania law with respect to any issues covered thereby. Subject to Section VI above, any action related to or arising from this Agreement with respect to a Participating State will take place exclusively in the courts situated in such state and the Parties hereby submit to the exclusive venue of the courts situated therein.

(p) Auditor and the Participating States hereby agree that they will keep this Agreement and its terms and conditions confidential and will not disclose such matters to any other persons or entities unless such disclosure is: (i) required by legal process or applicable law; (ii) made to a tribunal of competent jurisdiction for the purpose of enforcing obligations related to this Agreement; or (iii) made in confidence to their own attorneys, accountants or other professional advisers, to the extent such persons agree to keep such information confidential. Auditor and the Participating States agree not to issue any press releases containing the terms of this Agreement or otherwise disclose the terms of this Agreement unless required by law or court order.

IN WITNESS WHEREOF, the Parties have caused this Audit Resolution Agreement to be executed as of the date set forth above by their duly authorized representatives.

The [COMPANY NAME] COMPANY

By: _____

Date: _____

Its: _____

Audit Services U.S., LLC

By: _____

Date: _____

Its: _____

STATE NAME

By: _____

Date: _____

Its: _____

STATE NAME

By: _____

Date: _____

Its: _____

STATE NAME

By: _____

Date: _____

Its: _____

SCHEDULES AND EXHIBITS

Schedule A: Participating States

Schedule B: Specific Rules or Exceptions in Participating States

Exhibit 1: Form of Due Diligence Letter

SCHEDULE A
PARTICIPATING STATES

The following is a list of the Participating States in the unclaimed property audit that Auditor is conducting of Company:

1. STATE NAMES

SCHEDULE B

SPECIFIC RULES OR EXCEPTIONS IN PARTICIPATING STATES

1. **Dormancy Periods.** The Dormancy Periods for the Participating States are as follows:

State	IRA Dormancy Period
STATE NAME	3 years
STATE NAME	3 years
STATE NAME	3 years
STATE NAME	3 years

2. **De Minimis Exceptions.** No property shall be required to be reported or escheated to the following Participating States if the value of the property is equal to or less than the following amounts: STATE NAME

EXHIBIT 1
FORM OF DUE DILIGENCE LETTER

Date

Missing Owner Name

Missing Owner Last-Known Address

City, State Zip

THE STATE OF _____ REQUIRES US TO NOTIFY YOU THAT YOUR PROPERTY MAY BE REPORTED AS ABANDONED PROPERTY AND REMITTED TO THE CUSTODY OF THE STATE [COMPTROLLER/TREASURER] IF YOU DO NOT CONTACT US BEFORE MONTH DD, CCYY.

A recent review of our records indicates that we are holding the following property in your name that has remained inactive for an extended period of time or correspondence mailed to you has been returned as undeliverable by the United States Post Office:

Type(s) of Property:

Fund:

(optional) Account No.:

(optional) Total Value: \$_____ (as of Month DD, CCYY)

This value may vary with the fluctuation of financial market share prices.

The State of _____ has asserted that the above property is required to be delivered to the State unless you take the action outlined below.

- Sign, date and return this letter (see below).
 - If your current address is different than the one addressed on this letter, please provide us with your new address.
-

Upon receipt of this signed letter, we will record your continued interest in the property and reissue any outstanding checks to you.

We urge you to respond by Month DD, CCYY, to prevent the property from being potentially reported as unclaimed and transferred to the custody of the State of _____. If this occurs, you will be required to file a claim with the State's unclaimed property division to retrieve the property. Please note any shares may be sold by the state administrator. Additionally, IRS Revenue Rule 2018-17 (Withholding and Reporting with Respect to Payments from IRAs to State Unclaimed

Property Funds) is now effective. Under this ruling, the escheatment of a retirement account to the State may be subject to federal and state tax withholding rules.

If you have any questions, please contact our Shareholder Services department at 1 (XXX) XXX-XXXX.

Print your current address below if different from the address indicated above:

Signature

Date

If joint account, all owners must sign

Date

ASUS EXHIBIT O

Contractor
Assisted
Self-Audit

AUDIT SERVICES, U.S., LLC

CONTRACTOR ASSISTED SELF EXAMINATIONS

Upon prior written approval by the Program Manager, the Contractor may assist and/or oversee the process whereby a Holder performs a general ledger and/or securities self-examination. The Contractor does not generally take physical custody of the financial records of the Holder and does not perform an examination of those records. The Contractor informs the Holder of the requirements of the unclaimed property laws, details of the reporting requirements, provides the necessary information to the Holder or Holder's agent regarding unclaimed property and the reporting process and provides other necessary guidance and assistance to the Holder so that the Holder can accurately perform a self-examination. Upon the Holder's completion of the self-examination, the Contractor must review the unclaimed property report and ensure the report and remittance are submitted to UP after it has been determined by the Contractor to be complete, in the proper format and in compliance with the Act and voluntary disclosure program.

PLEASE NOTE:

The following **CONTRACTOR ASSISTED SELF EXAMINATION PLAN** was developed for the **State of Washington** and can easily be modified for use with the **State of West Virginia**.

ON STATE LETTERHEAD

Date

[Holder Name]

[Contact Name]

[Title]

[Mailing Address]

[City, State, Zip]

Dear [Mr./Ms. Contact Name]

The West Virginia State Treasury, Unclaimed Property Division under Chapter 36, Article 8 of the Uniform Unclaimed Property Act, of the West Virginia Code, is responsible for administering State's unclaimed property law. The primary goal of the unclaimed property law is to protect the rights of unclaimed property owners, which include businesses as well as individuals, and return as much of that property as possible to the rightful owners. Unclaimed property can include, but is not limited to: stock, uncashed checks, dormant bank accounts, insurance proceeds, security deposits, store credits and safe deposit box contents.

As part of our efforts to ensure that companies required to file an annual unclaimed property report (generally referred to as "Holders") are in compliance with Chapter 36, Article 8 of the Uniform Unclaimed Property Act, the West Virginia Unclaimed Property Division has established a Contractor Assisted Self Audit Program. This program enables companies to avail themselves of State authorized resources to facilitate compliance and resolve any apparent reporting deficiencies that may exist. All companies holding unclaimed property where the last known address of the owner is located in the State of West Virginia are subject to Chapter 36, Article 8 of the Uniform Unclaimed Property Act of the West Virginia Code.

Based on a review of our records, it appears that your company may have failed to file an unclaimed property report within the last three report years, or has met other review criteria, such as: missing common unclaimed property categories such as payroll or other general ledger related items. In order to confirm your compliance with Chapter 36, Article 8 of the Uniform Unclaimed Property Act, your company has been selected for the Contractor Assisted Self Audit Program. Your willingness to participate cooperatively in the program will weigh heavily on the State's decision to impose interest and penalties, as well as conduct a comprehensive field examination.

Audit Services US, LLC (ASUS) is an authorized service provider to the West Virginia Unclaimed Property Division with respect to this review. An ASUS representative will contact you within 10 business days to confirm your receipt of this notification and to answer any preliminary questions you might have. If you have any questions prior to being contacted or require further assistance, please contact the ASUS Support Desk at (PHONE NUMBER) or by email at (EMAIL ADDRESS). You may also contact [State Contact Person] or email [StateContact@WestVirginiaUnclaimed Property.Gov](mailto:StateContact@WestVirginiaUnclaimedProperty.Gov) at the West Virginia State Treasury, Unclaimed Property Division for further clarification as well.

If you believe that you received this notification in error or if you are not the party responsible for reporting your company's unclaimed property for the State's Unclaimed Property Division, please contact [Auditor Name] of ASUS at [Auditor Phone Number] or by email at AuditorName@auditservicesus.com

Sincerely,

[signature]

[title]



Contractor Assisted Self Audit (CASA) Holder Orientation Packet

West Virginia Office of the State Treasurer,
Unclaimed Property Division

Contractor Assisted Self-Audit Program

PAGE INTENTIONALLY LEFT BLANK

SAMPLE

CASA Holder Orientation Package

Table of Contents

I.	Cover Page.....	1
II.	Table of Contents.....	3
III.	Opening Teleconference Letter.....	4
IV.	Additional Disclosures.....	5
V.	Contractor Assisted Self Audit Action Items.....	6
VI.	Confidentiality Agreement.....	7
VII.	Self Audit Holder Questionnaire.....	8 - 10
VIII.	Opening Teleconference Agenda.....	11
IX.	Reporting Tools and Resources	
	a. Identifying Unclaimed Property and Data Collection.....	12 - 13
	b. Due Diligence.....	14 - 15
	c. Electronic Reporting.....	16
	d. Remittance Instructions.....	17
X.	West Virginia Office of the State Treasurer Unclaimed Property Section Guide to Reporting Unclaimed Property	
	a. West Virginia Property Category Code and Dormancy Table.....	18
	b. Owner and Relationship Codes.....	19-21
	c. Sample Due Diligence Letter.....	22



[Date]

[Holder Name]

[Contact Name]

[Title]

[Mailing Address]

[City, State Zip]

Dear [Mr./Ms. Contact Name]:

To assist you with complying with the [State Revised Statutes] and the procedures established for a Contractor Assisted Self Audit (CASA) program, we have included a CASA Holder Orientation Packet for your reference. Please review its contents at your earliest convenience.

Our responsibilities require Audit Services U.S., LLC, to gather and document basic corporate information. This will enable us to advise you on the types of property to be included in the Contractor Assisted Self Audit. We ask that you submit the completed Self-Audit Holder Questionnaire within 30 days of your receipt of this CASA Information Packet.

Once received, we will review the self-audit information prepared by your company and provide you guidance with respect to more detailed information gathering should that be necessary. Once all of the necessary information has been compiled and reviewed, Audit Services U.S. will assist you with the preparation of the state unclaimed property report. Upon completion of your final state unclaimed property report, we will perform a final review prior to you submitting the report and any unclaimed property that may be identified to the West Virginia Office of the State Treasurer, Unclaimed Property Division. You will be provided instructions on how to send the related property, i.e. cash and/or securities to a custodian.

Please note that participation in the CASA program does not exempt the holder from being audited in the future if the West Virginia Unclaimed Property Division deems an audit is warranted.

Please forward the Self-Audit Holder Questionnaire to Audit Services U.S., LLC via email to [Auditor Name] of Audit Services at AuditorName@auditservicesus.com.

Once we receive a completed Self-Audit Holder Questionnaire from you, [Auditor Name] of Audit Services U.S. will be contacting you within 10 days to set up an Opening Teleconference that allows us to discuss the CASA procedures and any other questions you may have about the process. In the meantime you may contact [Auditor Name] by phone at [Auditor Phone Number] or at the email referenced above.

We appreciate your continued cooperation and compliance.

Sincerely yours,

[signature]

[title]

ADDITIONAL DISCLOSURES

SENIOR CONTACT INFORMATION:

The Holder is free to discuss the audit directly with the liaison at any time regarding any questions or concerns relating to this review. Additional personnel listed below may also be contacted:

West Virginia Office of the State Treasurer, Unclaimed Property Division

Name: [State Contact Name]
Address: [State Address]
Phone: [State Phone Number]
Fax: [State Fax Number]
Email: [State Contact Email]

Audit Services U.S., LLC Contacts:

Jeremy Katz
Partner
Audit Services U.S., LLC
370 Lexington Avenue, Suite 707
New York, NY 10017
914-949-1570
Email: jkatz@auditservicesus.com

Contractor Assisted Self-Audit Action Items

- ☐ Holder mailed initial contact letter
- ☐ Holder Orientation Packet mailed
- ☐ Holder reviews contents of Holder Orientation Packet mailed by Audit Services U.S.
- ☐ Holder collects information to complete Self-Audit Holder Questionnaire.
- ☐ Audit Services U.S., LLC contacts Holder to schedule Opening Teleconference.
- ☐ Holder forwards Self-Audit Holder Questionnaire to Audit Services U.S., LLC
- ☐ Holder and Audit Services U.S., LLC conduct Opening Teleconference.
- ☐ Audit Services U.S., LLC provides CASA document request to Holder
- ☐ Upon completion of CASA document request, Holder and Audit Services U.S., LLC identify areas of company that generate unclaimed property and identify location of records.
- ☐ Audit Services U.S., LLC provides guidance to the Holder as needed.
- ☐ Holder collects unclaimed property records and converts to electronic format under close consultation from Audit Services U.S., LLC.
- ☐ Holder and Audit Services U.S. LLC analyzes unclaimed property records for dormancy requirements.
- ☐ Holder and Audit Services U.S. LLC analyzes "dormant" unclaimed property records for due diligence mailing requirements.
- ☐ Holder mails due diligence letters and allows for a minimum 60 day response period from owners/payees.
- ☐ Holder updates unclaimed property file to reflect owner/payee responses and any adjustments to produce a preliminary state unclaimed property report file.
- ☐ Holder forwards preliminary state unclaimed property report file to Audit Services U.S., LLC for review.
- ☐ Audit Services U.S., LLC sends notice to Holder to schedule Closing Teleconference.
- ☐ Holder and Audit Services U.S., LLC conduct Closing Teleconference.
- ☐ Holder generates Final State Unclaimed Property Report and sends to Audit Services U.S., LLC.
- ☐ Holder sends funds and/or securities in accordance with State reporting instructions.
- ☐ Audit Services U.S., LLC transmits Holder's Final State Unclaimed Property Report to the West Virginia Unclaimed Property Section and instructs custodian to forward funds and/or securities to the State.
- ☐ Audit Services U.S., LLC sends closing communication to Holder.

Confidentiality Agreement

[Date]

[COMPANY NAME]

Audit Services U.S., LLC (the "Contractor"), as agent for the **West Virginia Office of the State Treasurer, Unclaimed Property Division**, has requested certain information from [COMPANY NAME] (the "Holder") in connection with its unclaimed property review and audit of the Holder's books and records.

The Contractor shall treat as confidential and protect from disclosure to third parties, including other persons and business entities with whom the Contractor is affiliated, other than its own employees, agents, and representatives, and the States, all information that the Holder may furnish verbally and in writing to the Contractor or its agents, representatives, or employees in connection with its unclaimed property review and audit; provided however, that this letter agreement shall not prohibit the Contractor from disclosing such information to (a) any person specifically approved by the Holder or (b) pursuant to or as required by law. The Contractor further agrees that it will not use any such information for any purpose other than the performance of such review and audit.

The information referred to in the preceding paragraph shall not include any information (i) previously known to the Contractor prior to the receipt of such information, (ii) subsequently acquired by the Contractor from a third party having an independent right to disclose such information, or (iii) that is now or later becomes publicly known through no fault of the Contractor.

Any failure or delay by the Holder in enforcing any provision of this letter agreement will not operate as a waiver of that provision, and the Holder will be entitled to injunctive relief, as well as all other remedies available at law or equity, if the Contractor breaches this letter agreement.

This letter agreement constitutes the entire agreement between us and may only be modified in writing. This letter agreement and all controversies arising from it shall be governed by and construed in accordance with the laws of the State of West Virginia, without giving effect to its conflicts of law principles.

Sincerely,

Audit Services U.S., LLC

AGREED TO: [HOLDER]

Signature of Holder Representative: _____

Print Name: _____

Title: _____

TO BE COMPLETED BY [HOLDER]

West Virginia Office of the State Treasurer, Unclaimed Property Division**Self-Audit Holder Questionnaire**

Instructions: Please answer all questions on this form, and return to Audit Services U.S., LLC as soon as possible. If a question does not apply, please circle N/A (not applicable). **Please include a copy of your corporate organization chart with your response.**

Company Name:		Federal Employer ID No:
		Holder No:
Principal Administrative Office Address:		
State and Year of Incorporation:	Type of Business (financial, retail, manufacturing, etc):	Number of Employees:
		Total Revenue: \$
Contact Person Name:	Title:	Phone Number: () -
	Email Address:	Fax Number: () -

(Circle One)

Does your company have any uncashed, outstanding payroll checks older than ONE year? Yes No N/A

Does your company have any uncashed, outstanding payroll and/or commission checks older than THREE years? Yes No N/A

Does your company carry any uncashed outstanding checks issued to vendors, older than THREE years? Yes No N/A

Does your company maintain a reserve account for uncashed checks? Yes No N/A

Does your company offer a refund or rebate program? Yes No N/A

Has your company had any accounting system conversions? Yes No N/A

If yes, please indicate the month/year of conversion(s):

Was the employee benefit program established under a Federal Employee Retirement Income Security Act? Yes No N/A

Does your company offer a pension plan? Yes No N/A

Is there a trustee to administer and make disbursements for the company's pension plan? Yes No N/A

If yes, please indicate name and address of service:

Are outstanding pension checks accounted for and maintained by the trustee? Yes No N/A

Are payroll checks issued by a payroll service? Yes No N/A

If yes, please indicate name and address of service:

Does the payroll service account for and maintain uncashed payroll checks? Yes No N/A

Are there shareholders' accounts in undeliverable mail status and with dividends unpaid for three years? Yes No N/A

Are employee benefits paid through a union? Yes No N/A

If yes, please indicate union's name and address:

Does your company issue checks in a fiduciary capacity? Yes No N/A

If yes, please indicate the type of checks your company disburses for others:

Securities

(Circle One)

Are there amounts held for shareholders that did not redeem their shares?..... Yes No N/A

Did your company ever pay cash dividends, stock dividends, or interest on its debt (bonds)? Yes No N/A

Does your company hold any dividends for its shareholders that are unpaid and past due? Yes No N/A

Are there shareholders' accounts in undeliverable mail status and with dividends unpaid for three years? Yes No N/A

Does your company offer a dividend reinvestment plan? Yes No N/A

Does your company hold any unclaimed amounts due West Virginia resident payees? Yes No N/A

Company Changes

(Circle One)

Has your company undergone name changes, restructuring, etc.? Yes No N/A

If yes, please indicate the name of the companies AND corresponding FEIN #'s which were involved:

Has your company undergone mergers, acquisitions, etc.? Yes No N/A

If Yes, please indicate the name AND corresponding FEIN #'s of the companies which were involved:

Unclaimed Property Reporting History

(Circle One)

Has your company ever reported unclaimed property to any state? Yes No N/A

If yes, please indicate the name of the state or states:

Was the property reported with complete payee's name and address? Yes No N/A

Does your company report unclaimed property for West Virginia residents to another state or states? Yes No N/A

If yes, please indicate the name of the state or states:

Does your company hold unclaimed amounts for unknown payees? Yes No N/A

Were the amounts reported for unknown payee(s)? Yes No N/A

If yes, please indicate the name of the state or states:

Does your company report unclaimed property on behalf of others? Yes No N/A

If yes, please indicate the name of the companies AND corresponding FEIN #'s for which it files:

Does your company report unclaimed property through another company (parent or holding company)? Yes No N/A

If yes, please indicate the name of the company AND corresponding FEIN #'s which reports:

Prior Unclaimed Property Audits (if any)

(Circle One)

Was your company ever audited for unclaimed property by any state, third party vendor or CPA firm? Yes No N/A

Did the audit result in a supplemental filing with additional amounts due as unclaimed? Yes No N/A

Signature of Person Completing Form

Print Name

Title

Email

Phone

OPENING TELECONFERENCE AGENDA

Overview of Contractor Assisted Self-Audit Program

- Intro to Audit Services U.S., LLC and personnel
- Authorized by State of West Virginia to facilitate compliance for In-State and Out-of-State companies
- Good faith effort and cooperation may limit exposure to imposition of interest and penalties
- Self Audit by company – control of data collection
- Contractor will assist company with all aspects

Holder Overview

- Description of Business
 - Start Date
 - Type of Business
 - Customers
 - Vendors
 - Business Transactions
- Locations of Company records
- Format/availability of records
- History of unclaimed property reporting
 - Property Types
 - Years Reporting
- Any prior compliance issues

Unclaimed Property Rules-Contractor Assisted Self-Audit Program

- Identification of property types
- Assignment of property codes and relationship codes
- Electronic data conversion
- Analyze for dormancy and look back period
- Analyze for due diligence
- Send due diligence mailings and receive responses;
- Re-Issue or reactivate property
- Update Holder unclaimed property file
- Send unclaimed property file for review to Audit Services U.S., LLC
- Audit Services U.S., LLC will file Holder's unclaimed property report to the State
- Remit property to the designated custodian account for transfer to the State of West Virginia
- Assistance with other State compliance

Self-Audit Summary

- Holder completes analysis of company records and data collection
- Data conversion
- Completion of due diligence
- Information forwarded to Audit Services U.S., LLC
 - Description of Company Self-Audit Plan
 - Complete Reporting and Remittance
- Closing Conference

Tools Available

- West Virginia Unclaimed Property Reporting Instructions Manual (*Provided in HOP*)
- West Virginia Property Category Code and Dormancy Table (*Provided in HOP*)
- Relationship Code List (*Provided in HOP*)
- Electronic filing information – Sanctioned by NAUPA and the State of West Virginia
- File formats for conversion of Holder records
- Due diligence analysis with mailing options
- West Virginia Unclaimed Property website <http://www.State Name.gov/>



Holder Reporting Tools and Resources

Contractor Assisted Self-Audit Program

West Virginia Office of the State Treasurer
Unclaimed Property Division

[www.WestVirginia.gov/
UnclaimedProperty/HolderReporting/](http://www.WestVirginia.gov/UnclaimedProperty/HolderReporting/)

By Phone: [State Phone Number]
Email: ucpsupport@auditservicesus.com

Steps for Reporting and Remitting Unclaimed Property

- Identify the property to be reported and remitted i.e. property that has met

- the dormancy period.
- Perform Due Diligence on the unclaimed property to be reported and remitted.
- Prepare the unclaimed property report.
- Submit the unclaimed property report to Audit Services U.S., LLC, and remit the property.

Identifying Unclaimed Property and Data Collection

Unclaimed property is primarily an intangible property liability that has been inactive on the books of an entity for a period of time (**dormancy period**) for which there has been no owner generated activity. Unclaimed property is broadly defined and can include:

- Savings or Checking Accounts
- Stocks
- Uncashed Dividends
- Payroll checks
- Credits
- Traveler's Checks
- Trust Distributions
- Unredeemed Money Orders
- Unredeemed Gift Certificates (*not applicable in all states*)
- Insurance Payments or Refunds
- Life Insurance Policies
- Annuities
- Certificates of Deposit
- Customer Overpayments
- Utility Security Deposits
- Mineral Royalty Payments
- Safe Deposit Box Contents

Reaching the Dormancy Period

All unclaimed property must be reported and remitted to the West Virginia Unclaimed Property Section if the property has reached the required dormancy period.

There are different holding/dormancy periods per property type. Please refer to the West Virginia Property Category Code and Dormancy Table.

Review or "Look Back" Period

Holder compliance with the Contractor Assisted Self-Audit program requires the Holder to identify records that go back a minimum of 7 report years or all property held in the Holder's books and records that have met the dormancy period. This is called the *Look Back Period*.

Holders must demonstrate a good faith effort to collect and analyze all of their unclaimed property to be considered by the Department for a waiver of past due interest and penalties.

Suggested Checklist of Identifying Holder Unclaimed Property

☐ Basic Corporate Information Gathering/Site Selection:

Identify where all record-keeping, accounting and, if applicable, escheat reporting is performed to determine the particular entities, business units or Third-Party Administrators (TPA's) to be reviewed.

The following items should be considered:

- Annual reports to stockholders
- Financial Statements
- Organization chart setting forth the Holder's record-keeping, accounting, bank account and escheat reporting sites, with a description (e.g., revenues, headcount, business line) of the business and/or entities services by each site

- External and internal auditors – methodology for centralized or decentralized accounting procedures.
- Obtain current list (e.g., equity transfer and exchange agents; debt trustees; medical benefits, pension plans).
- Obtain list of changes in TPAs since 1985.

☐ The Holder's Look Back Period or Review Period

The Holder needs to determine the amount of abandoned property generated during the Look Back or Review Period. The Holder will determine the amount of outstanding liability related to the stale dated amounts contained in the Holder's presently maintained internal accounting system. Items to review could be the following:

Obtain the current chart of accounts to ascertain which accounts may relate to abandoned property. For example:

Unclaimed property
Escheatable property
Stale dated checks
Uncleared checks
Small balance write-offs
Suspense
Collections – undistributed
Write-offs – operating
Write-offs – payroll
Inactive customer accounts
Inactive escrow accounts
Inactive commission accounts

List of all bank accounts open, active or closed during the examination period

- Investigate changes in all accounts within the chart of accounts relating to abandoned property
- Determine Holder policies regarding stale dated checks and account balances:

- Payroll and Accounts payable
- Checks and drafts written for insurance claims
- Accounts receivable
- Write-offs
- Sales incentive programs (e.g., gift certificates, rebates)
- Benefit plans, defined benefit and defined contribution
- Self-insured programs (e.g., health plans, dental plans, workmen's compensation, general liability)

- Understand Holder's escheat accounting system, if applicable:

- Abandoned property policies & procedure manual
- Description of escheat system
- Summary of abandoned property filings, all states, latest available periods, by type of property
- Copies of prior unclaimed property reports for all states and supporting work papers for recent period
- Copies of unclaimed property audits and releases by state

Report Preparation

In accordance with the State of West Virginia Office of the State Treasurer Unclaimed Property Division Holder Reporting Manual reports must be remitted using the NAUPA standard format.

Detailed information on the NAUPA standard format can be found on Page 19 of the West Virginia Holder Reporting Manual.

HOLDER DUE DILIGENCE REQUIREMENTS AND DUE DILIGENCE MAILING PROCESS

Prior to reporting and remitting unclaimed property which has reached its required dormancy period for an applicable calendar year, West Virginia Statutes requires that for all the unclaimed property accounts valued at \$50.00 or greater, the holder must perform due diligence (Page 12 of the West Virginia Holder Reporting Manual.). A written notice is required to be sent to the apparent owner's last known address informing the apparent owner that the holder is in possession of the unclaimed property account and requesting that the apparent owner respond to the notice.

The holder must provide the name and contact information of the holder's staff person whom the owner can contact if they have any questions. To avoid confusion, the due diligence letter must not contain any contact information for the state. Failure to perform due diligence as provided by statute could result in potential fines and interest/penalties.

To complete the due diligence requirements for the Contractor Assisted Self-Audit program, the Holder must perform the following:

- 1) Analyze their unclaimed property file to determine those records that have met their dormancy period.
- 2) For those records that have met the dormancy period, a notice must be sent to any account (unclaimed property record) whose value is \$50.00 or greater. The written notice must be sent to the last known address of the owner on the Holder's records. A written notice is not required if there is a known bad address.
- 3) The Holder must allow no less than 60 days and no more than 120 days for returns of any owner/payee responses to the written notice.
- 4) The Holder must update their unclaimed property records to reflect valid owner responses if contact or activity has been established. The Holder should maintain records of owner responses from valid returned responses or other responses by an owner from phone contact or email.
- 5) When an adequate amount of time has elapsed, the Holder will need to provide a copy of the updated unclaimed property file to Audit Services U.S., LLC

DUE DILIGENCE MAILING OPTIONS

The Holder has various options to assist them with complying with the due diligence requirements.

- 1) Create, mail and track your own due diligence letters.
- 2) There are "Free" versions of software that support the creation of due diligence letters.
- 3) There are vendors that offer Due Diligence Mailing Services for a fee.*

***Notice: Audit Services U.S., LLC does not receive any consideration for fees earned by outside vendors.**

Due Diligence Letter Contents

Due diligence letters should include the following:

- Owner name
- Property description and amount
- Date of last activity with the owner
- Description of any action an owner must take to prove ownership and claim the property
- Date by which an owner must claim the property
- Your company's name, address, and contact's name, address, email, and phone number
- Date when the property will be reported to the state
- Statement that owners must claim property from state after it has been turned over (provide the state's web site)
- Provide a form where the owner can request for the property to be reactivated or have a check reissued, as well as provide the correct mailing address and any comments.

Holder Unclaimed Property Electronic Reporting

In accordance with the State of West Virginia Office of the State Treasurer Unclaimed Property Division Holder Reporting Manual reports must be remitted using the NAUPA standard format.

To assist you in creating the electronic report in the NAUPA standard format, NAUPA approved software programs are also available for free on the State's web page.

NOTE: The software programs mentioned above are provided by a third-party vendor, and the Department shall not be held responsible for any errors in the resulting report. It is the responsibility of the reporting entity to ensure the report is thoroughly reviewed for accuracy.

All reports must be filed online through the State web page [https://holder.West Virginiaunclaimedproperty.gov/](https://holder.WestVirginiaunclaimedproperty.gov/) reports not submitted online will be rejected.

Detailed information on the NAUPA standard format can be found on Page 19 of the West Virginia Holder Reporting Manual at **Error! Hyperlink reference not valid..**

Final unclaimed property reports must be sent to Audit Services U.S.. As part of the Contractor Assisted Self-Audit program, the Holder is responsible for copying Audit Services U.S. on all unclaimed property reporting applicable to the Contractor Assisted Self-Audit period(s).

Holder Unclaimed Property Remittance Instructions

- Instructions for Remitting Cash or Securities Property:
 - Cash – instructions to be provided upon completion of CASA review.
 - Securities and Mutual Funds

SECURITIES representing underlying shares, stock splits, bonds, etc., must be registered in our nominee name: West Virginia Unclaimed Property. For additional information, see below.

Any reports submitted to West Virginia Unclaimed Property that are not received in the proper format as defined by West Virginia law and this manual will be returned unprocessed, subject to penalty and interest, pursuant to [State Revised Statute].

Holders participating in DTC (Depository Trust Company) MUST transfer re-registered securities directly to:

Nominee Name: DTC Participant #123** West Virginia Unclaimed Property Agent Bank #45600** FEIN: 12-3456789 Account #987654***

Register Book Entry Shares/Direct Registration Shares (DRS)/Dividend Reinvestments Shares as follows:

Nominee Name: c/o Custodian for West Virginia
Unclaimed Property
[Street Address]
FEIN: 12-3456789
[City, State, Zip]

Fed Delivery: Federal Reserve Bank of New York
ABA #1234-0000-0
Big Bank
FBO—State of West Virginia Acct #781000

Detailed instructions for on-line reporting may be found at:

Error! Hyperlink reference not valid.



UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

WV Property Type Codes

Effective June 10, 2022

CODE	PROPERTY	YEARS
BANKS & FINANCIAL INSTITUTIONS		
AC01	Checking Accounts	5
AC02	Savings Accounts	5
AC03	Mature CD or Save Cert	5
AC04	Christmas Club Accounts	5
AC05	Money on deposit to secure funds	5
AC06	Security Deposits	5
AC07	Unidentified Deposits	5
AC08	Suspense Accounts	5
AC99	Aggregate Account balances	5
COLLEGE SAVINGS ACCOUNTS		
CS01	Cash	3
CS02	Mutual Funds	3
CS03	Securities	3
COURTS & GOVERNMENT ENTITIES		
CT01	Escrow Funds	1
CT02	Condemnation Awards	1
CT03	Missing Heir Funds	1
CT04	Suspense Accounts	1
CT05	Other Court Deposits	1
CT08	General Receiver accounts	1
CT09	Court Ordered Refunds/Restitution	1
CT13	Bonds deposited with the Court	1
CT99	Aggregate Court Deposits	1
DEMUTUALIZATION		
DM01	Cash	3
DM02	Stock	5
HEALTH SAVINGS ACCOUNTS		
HS01	Health Savings Account	3
HS02	Health Savings Account – Investment	3
INSURANCE		
IN01	Individual Policy Benefits or Claim Payments (Regardless of insurance type; does not include amounts reportable under IN03 o	3
IN02	Group Policy Benefits or Claim Payments (Regardless of insurance type; does not include amounts reportable under IN03 or IN	3
IN03	Amounts due beneficiaries from a life or endowment insurance policy or annuity	3
IN04	Amounts from matured or terminated life insurance policies, endowments or annuities	3
IN05	Premium Refunds (Includes all other life insurance premium refunds not covered by IN04)	3
IN06	Unidentified Remittances	3
IN07	Other Amounts Due Under Policy Terms	3
IN08	Agent Credit Balances	1
IN99	Aggregate Insurance Property	3
TRADITIONAL IRA, SEP IRA, SARSEP IRA AND SIMPLE IRA'S		
IR01	Cash	3
IR02	Mutual Funds	3
IR03	Securities	3
ROTH IRA'S		
IR05	Cash	3
IR06	Mutual Funds	3
IR07	Securities	3
LAW ENFORCEMENT		
LE01	Law Enforcement - Cash	6 months
LE98	Law Enforcement – Tangibles	6 months





UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

CODE	PROPERTY**	YEARS
MINERAL PROCEEDS AND MINERAL INTERESTS		
MI01	Net Revenue Interests	3
MI02	Royalties	3
MI03	Overriding Royalties	3
MI04	Production Payments	3
MI05	Working Interests	3
MI06	Bonuses	3
MI07	Delay Rentals	3
MI08	Shut-in Royalties	3
MI09	Minimum Royalties	3
MI99	Aggregate Mineral Proceeds	3
MISCELLANEOUS CHECKS AND INTANGIBLE PERSONAL PROPERTY		
MS01	Wages, payroll, or salary	1
MS02	Commissions	1
MS03	Workers' Compensation Benefits	1
MS04	Payments for Goods and Services	3
MS05	Customer Overpayments/Credit Balances--Retail only	3
MS06	Unidentified Remittances	3
MS07	Unrefunded Overcharges	3
MS08	Accounts Payable	3
MS09	Credit Balances/Accounts Receivable	3
MS10	Discounts Due	3
MS11	Refunds due	3
MS12	Unredeemed Gift Certificates	3
MS13	Unclaimed Loan Collateral	3
MS14	Pension and Profit Sharing Plans (IRA, KEOGH, e.g.)	3
MS15	Dissolution or Liquidation Funds	1
MS16	Miscellaneous Outstanding Checks	3
MS17	Miscellaneous Intangible Property	3
MS18	Suspense Liabilities	3
MS99	Aggregate Misc Property	3
SAFE DEPOSIT BOXES AND SAFEKEEPING		
SD01	Contents of safe deposit boxes	5
SD02	Contents of any other safekeeping repository	5
SD03	Other Tangible Property	5
SD04	Safe Deposit - Proceeds from the sale of contents	5
SECURITIES		
SC01	Dividends	5
SC02	Interest (Bond Coupons)	5
SC03	Bond Principal	5
SC04	Equity Payments	3
SC05	Profits	3
SC06	Funds Paid to Purchase Shares	3
SC07	Funds for Stocks and Bonds	3
SC08	Shares of Stock (returned by post office)	5
SC09	Cash for Fractional Shares	3
SC10	Unexchanged Stock of Successor Corporation	5
SC11	Other Certificates of Ownership	5
SC12	Underlying Shares	5
SC13	Funds for Liquidation/Redemption of Unsurrendered Stocks or Bonds	3
SC14	Debentures	3
SC15	U.S. Government Securities	5
SC16	Mutual Fund Shares	5
SC17	Warrants (Rights)	3
SC18	Mature Bond Principal	5
SC19	Dividend Reinvestment Plans	5
SC20	Credit Balances	3
SC21	Liquidated Mutual Fund Shares	3
SC99	Aggregate Security Related Cash	





UNCLAIMED PROPERTY

West Virginia State Treasurer's Office

CODE	PROPERTY**	YEARS
TRUST, INVESTMENTS, AND ESCROW ACCOUNTS		
TR01	Paying Agent Accounts	3
TR02	Undelivered or Uncashed Dividends	3
TR03	Funds held in Fiduciary Capacity (such as, trust, guardian, estate, etc.)	3
TR04	Escrow Accounts	3
TR05	Trust Vouchers	3
TR99	Aggregate Trust Property	3
UNCASHED CHECKS		
CK01	Cashier's Checks	3
CK02	Certified Checks	3
CK03	Registered Checks	3
CK04	Treasurer's Checks -- West Virginia Checks (6 Month Dormancy), All Other Checks (3 Year Dormancy)	6 ms or 3
CK05	Drafts	3
CK06	Warrants	3
CK07	Money Orders -- Financial Institutions (3 Year Dormancy), Entities other than Financial Institutions (7 Year Dormancy)	3 or 7
CK08	Traveler's Checks	15
CK09	Foreign Exchange checks	3
CK10	Expense Checks	3
CK11	Pension Checks	3
CK12	Credit Checks or Memos	3
CK13	Vendor Checks	3
CK14	Checks Written off to Income or Surplus	3
CK15	Other Outstanding Official Checks or Exchange Items	3
CK16	CD Interest Checks	3
CK99	Aggregate Uncashed Checks	3
UTILITIES		
UT01	Utility Deposits	1
UT02	Membership Fees	1
UT03	Refunds or Rebates	1
UT04	Capital Credit Distributions	3
UT99	Aggregate Utilities	1
Virtual Currency		
VC02	Virtual Currency Liquidated	3

Public Agencies - Use the most applicable property type code and report all property with one (1) year dormancy.



Sample Due Diligence Letter

SAMPLE



Report Year 2019

<https://nevadatreasurer.gov/>

Sample Due Diligence Letter

Due Diligence

Acme Funds Corporation
123 Abandoned Lane
Anywhere USA 12345

Date

Owner Name
456 Asset Road
Jackpot USA 67890

Re: Account #
Balance \$
Property Type:

Dear Owner:

We are holding unclaimed property with a value of at least \$50 for the person listed above. The owner may claim this property by contacting us at the address or phone number listed below.

Holder Information: Company Name
Address
Phone #

Failure to respond by *(insert the last day property will be available for refund)*, will result in property being remitted to Nevada Unclaimed Property by October 31st *(April 30th for all insurance entities)*. After that date, the owner may contact the state where the property will be held in perpetuity and can be rightfully claimed.

Sincerely,

Company's Contact Person's Name

ASUS EXHIBIT P

Sample
Holder
Profile

Hertz Global Holdings, Inc.

Business Description:

Headquarters Address:

8501 Williams Rd., Ste. 3
Estero, FL 33928-3325

Phone: (239) 301-7000

Fax: N/A

Website: www.hertz.com

Key Company Facts:

Industry: Automobile Renting

Company Type: Public

FEIN: 20-3530539

Fiscal Year-End: 12/31

Sales: \$9.8 Billion

Employees: 38,000

Year Started: 1918

Incorporation Date: 8/28/2015

State of Incorporation: DE

Independent Auditor: N/A

Hertz Global Holdings, the parent company of The Hertz Corporation, was ranked 335th in Forbes' 2018 Fortune 500 list. As of 2019, the company had revenues of US\$9.8 billion, assets of US\$24.6 billion, and 38,000 employees. The company filed for bankruptcy on May 22, 2020, citing a sharp decline in revenue and future bookings caused by the COVID-19.

Established in 1918, the Hertz Corporation, a subsidiary of Hertz Global Holdings, Inc., is an American car rental company based in Estero, Florida, that operates 10,200 corporate and franchisee locations internationally.

Audit Objective: To review the Holder's books and records to identify unclaimed property due and payable prior to the May 22, 2020 effective date of their filing for Chapter 11 protection.

Ownership: Hertz Corporation is owned by Hertz Global Holdings, Inc.

Officers:

Paul E. Stone, President, CEO

Jamere Jackson, Exec. V.P., CFO

Richard E. Esper, Sr. V.P., Chief Accounting Officer

M. David Galainena, Exec. V.P., General Counsel & Secretary

Previous Names: None

Subsidiaries (Including but not limited to):

1. Hertz Corporation
2. Dollar Rent-A-Car
3. Firefly Car Rental
4. Thrifty Car Sales, Inc.

ASUS EXHIBIT Q

Sample
Invoice

For Illustrative Purposes Only



Audit Services, U.S., LLC
370 Lexington Avenue, Suite 707
New York, NY 10017

Services Rendered For Auditing:

ABC Company
XYZ Inc
123 Broadway
New York, NY 10001

STATE WEST VIRGINIA
INVOICE # WV000781
DATE 4/29/2022

Shares Delivered via DTC: 1,500

12-3456789

Share Description	Shares	Share Value	Total Billable Share Value	Cash	Total Billable Property Value
Cash Reported				\$ 10,000.00	\$ 10,000.00
Shares Reported	1,500	\$ 10.00	\$ 15,000.00		\$ 15,000.00
TOTALS	1,500		\$ 15,000.00	\$ 10,000.00	\$ 25,000.00
1. Amount Reportable to State:					\$ 25,000.00
2. ASUS Services Fee (10.5%)					\$ 2,562.50
3. Amount Due					\$ 2,562.50

If you have any questions regarding
the above, please contact us at:

Audit Services, U.S., LLC
370 Lexington Avenue, Suite 707
New York, NY 10017
Phone: 212-594-5487
Fax: 212-594-5571

Please send remittance to:

Audit Services, U.S., LLC
370 Lexington Avenue, Suite 707
New York, NY 10017



For Illustrative Purposes Only

Audit Services U.S., LLC
370 Lexington Avenue, Suite 707
New York, NY 10017
Phone: 212-594-5487
Fax: 212-594-5571

April 29, 2022

Heather D. Harrison
West Virginia State Treasury
Unclaimed Property Division
PO Box 4228
Charleston, WV 25364

Dear Heather:

Attached please find the following:

Invoice Number:	WV000781
Invoice Amount:	\$2,562.50

For services rendered auditing:

Company Name / CUSIP:	ABC Company	123456789
Acquired Company / CUSIP:	XYZ Inc	987654321
Address 1:	123 Broadway	
Address 2:	New York, NY 10001	
Address 3:		
FEIN:	12-3456789	

Event Date:	1/1/2001
Cash Exchange Rate:	N/A
Share Exchange Rate:	1.50000
Cash for Fractional Shares:	\$7.50000

Shares Remitted:	1,500	0
Cash Remitted:	\$10,000.00	See enclosed check

Value of Property Reported:	\$25,000.00
------------------------------------	--------------------

If you need additional information, please do not hesitate to contact me.

Sincerely,

Matt Thornton
Chief Operating Officer
Audit Services, U.S., LLC

ASUS EXHIBIT R

Sample
Work-In-Progress
Report



ASUS Exhibit R

Work in Progress Report for the State of West Virginia
For the Period Ending August 31, 2022

AUDIT ID	VENDOR	HOLDER NAME	PROJECT- GL, SECURITIES, AR, AP, ETC	FEIN
0001234	ASUS	ABC COMPANY	GENERAL LEDGER	123456789
0002345	ASUS	XYZ CORPORATION	GENERAL LEDGER	234567890

LAST ACTIVITY DATE	STATUS	HOLDER ADVOCATE	LEGAL REPRESENTATIVE	AUDIT APPROVED
4/21/2022	3.a_Audit review in process	11	22	1/19/2022
4/29/2022	3.a_Audit review in process	33	44	1/21/2022

OPENING CONFERENCE	NDA	INITIAL RECORDS DELIVERED	MOST RECENT RECORDS DELIVERED	% COMPLETED
2/22/2022	2/25/2022	3/1/2022	4/1/2022	30
2/14/2022	2/21/2022	3/15/2022	4/12/2022	20

PRELIMINARY FINDINGS	FINAL FINDINGS PRESENTED	REPORT UPLOADED	FUNDS DELIVERED	AUDIT CLOSED

NOTE/COMMENTS