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 5

List View

General Information | Contact | Default Values | Discount | Document Information | Clarification Request

Procurement Folder: 2028979
Procurement Type: Central Master Agreement
Vendor ID: VS0000047408
Legal Name: Consultadd Inc.
Alias/DBA:
Total Bid: $334,400.00
Response Date: 08/24/2026
Response Time: 10:53
Responded By User ID: Jessicasmith
First Name: Jessica
Last Name: Smith
Email: jessica.s@consultadd.com
Phone: 8887719958

SO Doc Code: CRFQ
SO Dept: 0231
SO Doc ID: OOT2700000005
Published Date: 8/18/26
Close Date: 8/25/26
Close Time: 13:30
Status: Closed
Solicitation Description: Addendum No 1-Advanced Email Security
Total of Header Attachments: 5
Total of All Attachments: 5

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:	2028979
Solicitation Description:	Addendum No 1-Advanced Email Security
Proc Type:	Central Master Agreement

Solicitation Closes	Solicitation Response	Version
2026-08-25 13:30	SR 0231 ESR08242600000001238	1

VENDOR

VS0000047408
Consultadd Inc.

Solicitation Number: CRFQ 0231 OOT2700000005

Total Bid: 334400 **Response Date:** 2026-08-24 **Response Time:** 10:53:45

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	Core Detection	22000.000	EA	3.700000	81400.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
2	Core Detection - Year 2 (Optional Renewal)	22000.000	EA	3.700000	81400.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
3	Core Detection - Year 3 (Optional Renewal)	22000.000	EA	3.900000	85800.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Ln Total Or Contract Amount
4	Core Detection - Year 4 (Optional Renewal)	22000.000	EA	3.900000	85800.00

Comm Code	Manufacturer	Specification	Model #
43230000			

Commodity Line Comments:

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

consultadd

Consultadd Inc.

SOC 2 TYPE II Report

For The Period,
January 01, 2025 to June 30, 2025

Independent Service Auditors' Report on Management's Description of a Service Organization's System Relevant to Security, Confidentiality and Availability and the Suitability of the Design and Operating Effectiveness of Controls

accorp

Prepared by: **Accorp Partners**

Table of contents

SECTION 1

INDEPENDENT SERVICE AUDITOR'S REPORT

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 Relevant to Security, Confidentiality and Availability

To: Management of Consultadd Inc. (Consultadd)

Scope

We have examined Consultadd Inc.'s accompanying description of its Consultadd system found in Description of System, Section 3 titled "Consultadd Inc. powers businesses with smart tech consulting and agile talent solutions" throughout the period January 01, 2025 to June 30, 2025 (description) based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria, (description criteria) and the suitability of the design and operating effectiveness of controls stated in the description throughout the period January 01, 2025 to June 30, 2025, to provide reasonable assurance that Consultadd'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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria.

As indicated in the description, Consultadd does not use any subservice organization for providing business process outsourcing.

The Description also indicates that Consultadd's controls can provide reasonable assurance that certain service commitments and system requirements can be achieved only if complementary user entity controls assumed in the design of Consultadd'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 and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Consultadd 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 Consultadd's service commitments and system requirements were achieved. In Management Assertion, Section 2, Consultadd has provided the accompanying assertion titled "Assertion of the Management of Consultadd Inc." about the description and the suitability of design and operating effectiveness of controls stated therein. Consultadd 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 AICPA. 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.

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

An examination of a description of a service organization’s system and the suitability of the design and operating effectiveness of controls involves—

- 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.
- 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. 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 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 listed in section 4 of our report titled "Independent Service Auditors' Description of Test of Controls and Results".

Opinion

In our opinion, in all material respects—

a. the description presents Consultadd's system that was designed and implemented throughout the period January 01, 2025 to June 30, 2025 in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period January 01, 2025 to June 30, 2025 to provide reasonable assurance that Consultadd'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 if the user entities applied the complementary controls assumed in the design of Consultadd's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period January 01, 2025 to June 30, 2025 to provide reasonable assurance that Consultadd's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Consultadd's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4 of this report, is intended solely for the information and use of Consultadd; user entities of Consultadd's system during some or all of the period January 01, 2025 to June 30, 2025, business partners of Consultadd subject to risks arising from interactions with the Consultadd 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, and other parties.
- Internal control and its limitations.
- Complementary user-entity 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.
- 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 the specified parties.

Accorp Partners CPA LLC
License No.: PAC-FIRM-LIC-47383
Kalispell, Montana

SECTION 2

MANAGEMENT ASSERTION

Assertion of the Management of Consultadd Inc.

We have prepared the accompanying description of Consultadd Inc.'s (Consultadd) system titled Consultadd Inc. powers businesses with smart tech consulting and agile talent solutions throughout the period January 01, 2025 to June 30, 2025 (description) based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)*, in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Consultadd system that may be useful when assessing the risks arising from interactions with Consultadd's system, particularly information about system controls that Consultadd 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality and Privacy (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

Consultadd does not use any subservice organization for providing business process outsourcing.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Consultadd, to achieve Consultadd'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 complementary user entity controls assumed in the design of the service organization's controls.

We confirm, to the best of our knowledge and belief, that

1. The description presents Consultadd system that was designed and implemented throughout the period January 01, 2025 to June 30, 2025 in accordance with the description criteria.

2. The controls stated in the description were suitably designed throughout the period January 01, 2025 to June 30, 2025 to provide reasonable assurance that Consultadd'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 if the user entities applied the complementary controls assumed in the design of Consultadd's controls throughout that period.

3. The controls stated in the description operated effectively throughout the period January 01, 2025 to June 30, 2025 to provide reasonable assurance that Consultadd's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary user entity controls assumed in the design of Consultadd's controls operated effectively throughout that period.

Sincerely,

Aukit Pathak

Ankit Pathak

CEO

SECTION 3

SYSTEM DESCRIPTION

Background and Overview of Services

Company Background

Consultadd Inc. is a technology consulting and talent solutions company that helps startups and enterprises solve complex problems through software development, cloud services, data engineering, and IT staffing. Headquartered in the U.S., the company operates globally with a strong focus on innovation, agility, and client success across industries like finance, healthcare, and retail. Consultadd's services and controls are also designed to meet the expectations of public sector clients, including government agencies, educational institutions, and municipalities that require high levels of security, confidentiality, and availability.

Description of Services provided

- Software Development
- Cloud Services
- Data Engineering
- IT Staffing
- DevOps Consulting
- Business Intelligence
- QA & Testing
- UI/UX Design
- Mobile App Development
- Agile Transformation
- Technology Training & Upskilling
- IT Strategy Consulting
- IT Managed Service
- Staff Augmentation
- Cybersecurity Services
- ERP Implementation
- CRM Implementation

Subservice Organizations

Consultadd does not use any Subservice Organization to provide services to its clients. Consultadd resources work in client's cloud environment.

Principal Service Commitments and System Requirements

Consultadd designs its processes and procedures related to the System to meet its objectives. Those objectives are based on the service commitments, related laws and regulations of products and services, and financial, operational, and other compliance requirements that have been established for such services. Security commitments to user entities are documented and communicated in customer agreements, as well as in the description of the service offering provided online. Consultadd establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such

requirements are communicated in Consultadd's system policies and procedures, system design documentation, and contracts with customers.

Information security policies define an organization-wide approach as to how the 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 the System.

Components of the System

The System is comprised of the following components:

- Infrastructure including the physical structures, Information Technology (IT), and other hardware.
- Software including application programs and IT system software that support the business operations.
- People including executives, sales and marketing, client services, customer support, information processing, software development, IT, Finance, and Human resources.
- Procedures (automated and manual).
- Data including transaction streams, files, databases, tables, and output used or processed by the system.

The System boundaries include the applications, databases, and infrastructure required to directly support the services provided to Consultadd's clients. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to Consultadd's customers are not included within the boundaries of its system.

Boundaries of the System

The specific products, services, and locations that are included in the scope of the report are given below. All other products, services, and locations are not included.

Products and Services in Scope	
Services • Software Development • Cloud Services • Data Engineering • IT Staffing • DevOps Consulting • Business Intelligence • QA & Testing • UI/UX Design • Mobile App Development • Agile Transformation • Technology Training & Upskilling • IT Strategy Consulting • IT Managed Service • Staff Augmentation • Cybersecurity Services • ERP Implementation • CRM Implementation	
Geographic Locations in Scope	
USA	175 Greenwich St, 38th Floor, New York, NY, US, 10007
India	Floor No.4th, Wing B, International Tech Park, Grant Road, Pune, Maharashtra 411014

All the above material activities and operations in scope are performed from the above office location. Unless otherwise mentioned, the description and related controls apply only to the location covered by the report.

Description of Control Environment, Control Activities, Risk Assessment, Monitoring and Information, and Communication

Control Environment

Consultadd's internal control environment reflects the overall attitude, awareness, and actions of management concerning the importance of controls, and the emphasis given to controls in the Company's policies, procedures, methods, and organizational structure.

The Chief Executive Officer, the Senior Management Team, and all employees are committed to establishing and operating an effective Information Security Management System in accordance with its strategic business objectives. The Management is committed to the Information Security Management System and ensures that IT Security policies are communicated, understood, implemented, and adhered to at all levels of the organization and regularly reviewed for continual suitability.

Integrity and Ethical Values

Consultadd requires directors, officers, and employees to observe high standards of business and personal ethics in conducting their duties and responsibilities. Honesty and integrity are core principles of the Company, and all employees are expected to fulfill their responsibilities based on these principles and comply with all applicable laws and regulations. Consultadd promotes an environment of open communication and has created an environment where employees are protected from any kind of retaliation should a good-faith report of an ethics violation occur. Executive management has the exclusive responsibility to investigate all reported violations and to take corrective action when warranted.

Management's Philosophy and Operating Style

The Executive Management team assesses risks prior to venturing into business ventures and relationships. The Executive Management team to interact with operating management on a daily basis.

Risk Management and Risk Assessment

Risk assessments are performed annually to identify current risk levels, with recommendations to minimize those risks that are determined to pose an unacceptable level of risk to Consultadd. As part of this process, security threats are identified and the risk from these threats is formally assessed.

Consultadd has operationalized a risk assessment process to identify and manage risks that could adversely affect their ability to provide reliable processing for User Organizations. This process consists of the Information Security team identifying significant risks in their areas of responsibility and implementing appropriate measures to address those risks.

The following steps are involved in performing risk assessments

- Risk identification for each asset in a process and at the Organizational level.
- Risk analysis & evaluation for each asset in a process & at the Organizational level.
- Risk treatment & residual risk.

Risk assessment comprises calculating the level of risk associated with assets belonging to a particular business process. It is done in a manner to assess and evaluate the criticality of impact on business by a particular risk and also to identify the areas where the organization needs to focus on information security. Apart from the asset-based risk assessment, the Company has also conducted organization-based risk assessment which is based on internal as well as external issues, needs, and expectations of interested parties, etc. The threats, and vulnerabilities associated with every asset are evaluated along with threat impact, probability of occurrence, and chances of detection (on a rating basis) of the threat. This determines the Risk Factor, which is then put into an equation to derive a risk value. The risk value is then compared to the organizational threshold (i.e., accepted risk value) which is treated appropriately (i.e., treat, transfer, avoid, accept). The identified risks will be treated (mitigated) so that risk levels are reduced. The output of a risk assessment will include a complete risk register and risk treatment plan. Any action plans are tracked to completion. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changes in business conditions. Management and Information Security personnel monitor the quality of internal control performance as a routine part of their activities. Performance monitoring reports cover server parameters such as disc space, incoming/outgoing network traffic, packet loss, etc. These system performance reports are reviewed by management on a periodic basis. In addition, a self-assessment scan of vulnerabilities is performed on a yearly basis. Vulnerabilities are evaluated

and remediation actions are monitored and completed. Results and recommendations for improvement are reported to management.

Information and Communication

Consultadd has documented procedures covering significant functions and operations for each major work group. Policies and procedures are reviewed and updated based on suggestions from security personnel and approval by management. Departmental managers monitor adherence to policies and procedures as part of their daily activities. The management holds departmental status meetings, along with strategic planning meetings, to identify and address service issues, customer problems, and project management concerns. The CTO is the focal point for communication regarding the IT environment. Additionally, there are personnel that have been designated to interface with the customer if processing or systems development issues affect customer organizations. Electronic messaging has been incorporated into many of Consultadd's processes to provide timely information to employees regarding daily operating activities and to expedite management's ability to communicate with employees.

Electronic Mail (e-Mail)

Communication to Customer organizations and project teams is through e-mail. Important corporate events, employee news, and cultural updates are some of the messages communicated using e-mail. E-mail is also a means to draw the attention of employees towards adherence to specific procedural requirements. Consultadd requires two-factor authentications from employees to access their e-mails.

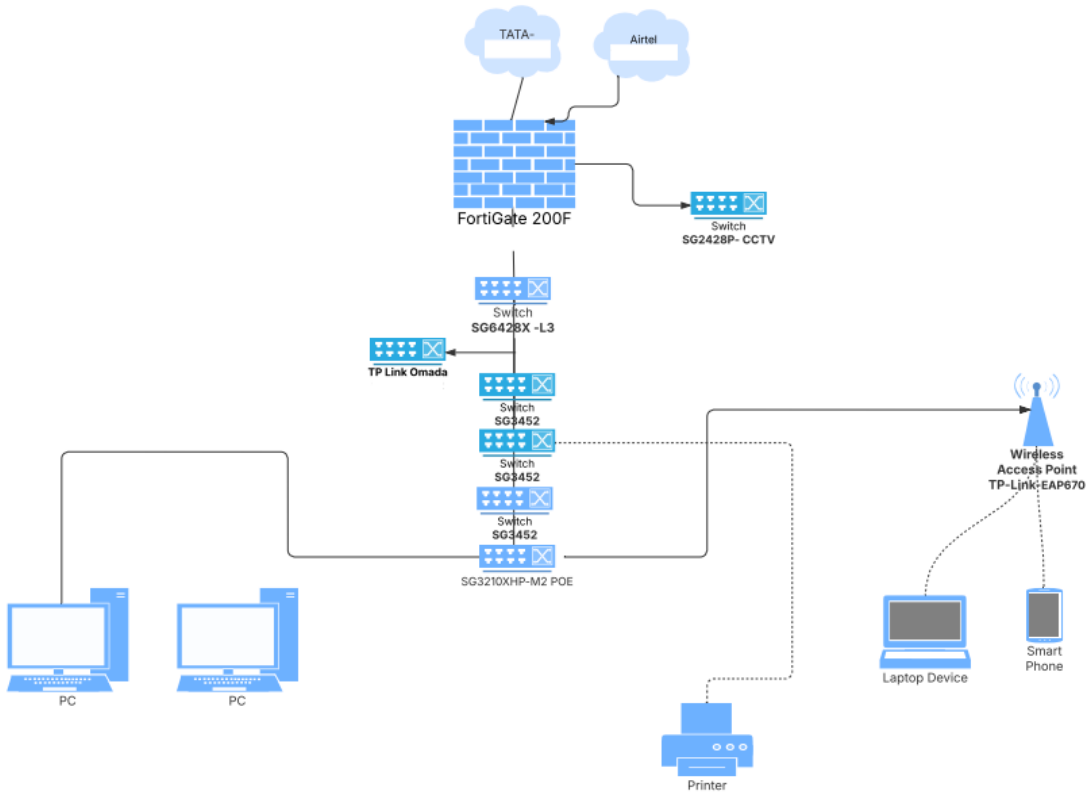
Components of the System

Infrastructure

The infrastructure comprises physical and hardware components of the System including facilities, equipment, and networks.

Network Segmentation Overview

Consultadd's offices are equipped with the latest hardware, software, and networking infrastructure. All the offices are linked through high-speed communication channels, backed up by redundant networks.



Software

Firewalls

The organization configures the FortiGate 200F physical firewall with strict access controls and monitors it comprehensively. The firewall is regularly updated and patched, included in incident response plans, and subject to regular audits, backups, and user training to maintain security and compliance.

Any change to configuration is overseen by the IT Security team. All configuration, backup and rules have been documented for compliance.

Network & Endpoint Protection

All systems and devices are protected by the comprehensive endpoint protection system. The endpoints include antivirus, anti-malware, and Trojan protection from any source. This also includes the e-mail scanning of the systems which prevents malicious scripts and viruses from the e-mails. Apart from this, all systems are restricted to the internet with the content filtering system routed through the proxy server.

Monitoring

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Consultadd'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 are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Consultadd'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, internal conference calls, and informal notifications.

Management's close involvement in Consultadd'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. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Consultadd's personnel.

Capacity Management

Capacity management controls are put in place so as to monitor, tune and project certain Consultadd's resources to ensure system performance meets the expected service levels and minimize the risk of systems failure and capacity-related issues. The addition of new information systems and facilities, upgrades, new versions, and changes are subject to formal system analysis, testing, and approval prior to acceptance.

Patch Management

The patch management activity is done regularly or as and when any critical event occurs and required updates or patches are installed to ensure efficient working of the servers, desktops, and critical network devices. Operating system patches related and marked critical, and security are managed and applied as they become available, windows systems are managed through the patch management system, and the network device's OS patching is managed automatically while renewing.

Vulnerability Scans & Security Audits

As per the Audit calendar, all the network devices and services are audited for vulnerabilities by doing periodic vulnerability scans. These scans are done by the internal IT Infrastructure team.

Virus Scans and Endpoint Security

Consultadd ensures antivirus is installed with the feature of scanning the device automatically in all the systems and log reports are reviewed by the IT Head. Updates to the virus definition files are managed and downloaded by the software itself on a daily basis from the vendor website at specific intervals.

People

Organizational Structure

The organizational structure provides the overall framework for planning, directing, and controlling operations. It has segregated personnel and business functions into functional groups according to their job responsibilities. This approach helps to enable the organization to define responsibilities, lines of reporting, and communication and helps facilitate employees to focus on the specific business issues impacting clients.

The management team meets regularly to review business unit plans and performances. Meetings with the CEO and department heads are held to review operational, security, and business issues, and plans for the future.

Consultadd's Information Security policies define and assign responsibility/accountabilities for information security. Regular management meetings are held to discuss the security level, changes, technology trends, occurrence of incidents, and security initiatives.

The following are the responsibilities of key roles.

- **Executive management** - Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- **Human resources (HR)** - Responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g., talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- **IT Security** – Responsible for Information Security including implementing, managing, and monitoring the information security program along with IT Risk Management.
- **IT** - Responsible for installation, configuration, operation, monitoring, and maintenance of IT.

Processes 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 Consultadd policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Consultadd team member.

Administrative Level Access

Administrative rights and access to administrative accounts are granted to individuals that require that level of access in order to perform their jobs. All administrative level access, other than to IT team, must be justified to and approved by IT team.

Confidentiality

Secure procedures are established to ensure safe and secure disposal of media when no longer required. The level of destruction or disposal of media would depend on the information or data stored in the media and the criticality of the information as per the information classification guideline.

Backup and Recovery of Data

Consultadd has developed formal policies and procedures relating to backup and recovery. Backup is defined in the Backup Policy. Suitable backups are taken and maintained. The backup processes are approved by the business owners and comply with the requirements for business continuity, and legal & regulatory requirements. All backup and restoration logs are maintained for retention periods as defined in the "Backup Policy".

Applicable Trust Services Criteria and related Controls

The Security, Confidentiality and Availability trust services categories and Consultadd related controls are included in section 4 of this report, "Independent Service Auditor's Description of Tests of Controls and Results".

Complimentary User-Entity Control Considerations

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria 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 are responsible for understanding and complying with their contractual obligations to Consultadd.
2. User entities are responsible for notifying Consultadd of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Consultadd services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Consultadd services.
6. User entities are responsible for providing Consultadd with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Consultadd of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

SECTION 4

DESCRIPTION OF TEST OF CONTROLS AND THEREOF

Trust Services Security, Confidentiality and Availability, Criteria & Related Controls and Test of effectiveness and Results of Test

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
Control Environment			
CC1.1	**COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.**		
	The Company has a mission and vision statements. Additionally, the entity has developed a clearly articulated statement of ethical values that is understood at all levels of the organization. The communication Mission, Vision and Ethical statement is through shared drive screenshot.	Inspected Induction PPT to determine that mission and vision statements of ethical values are established.	No Exceptions Noted
	The Company has approved code of conduct that is applied across the entity. Code of Conduct policy is posted on the shared directory and GRC Platform. The Code of Conduct outlines strict disciplinary consequences for violation of code of conduct	Inspected Code of Conduct on shared directory and GRC Platform to determine that Code of Conduct outlines strict disciplinary consequences for violation of code of conduct.	No Exceptions Noted
	All new employees are provided training and are made to sign Code of Conduct (CoC). New employees sign off that they have read this document. Existing employees, on an annual basis, undergo refresher training on Company's policies on code of conduct. COC posted on the shared directory	Inspected Induction training deck to determine that CoC training is given to all employees at least once a year.	No Exceptions Noted
	Performance appraisals are performed at least annually.	Inspected HR Process Handbook to determine that Performance appraisals are performed at least annually.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	Verified Non-Disclosure Agreement of sampled vendor to determine that confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	No Exceptions Noted
	The entity has code of conduct within the HR Policies that establishes standards and guidelines for personnel ethical behaviour. Personnel are required to read and accept the entity's code of conduct	Inspected the code of conduct policies to determine that the entity has established standards and guidelines for personnel ethical behaviour including code of conduct.	No Exceptions Noted
	All new employees have to read and sign the Confidentiality Agreement/NDA upon joining.	Selected a sample of new joiners and inspected personnel files to determine that Confidentiality agreements / NDAs are signed.	No Exceptions Noted
	Agreements are established with third parties or subcontractors that include clearly defined terms, conditions, and responsibilities for third parties and subcontractors.	Selected a sample and inspected the vendor agreements to determine that the agreements define the terms, conditions, and responsibilities of these vendors and their subcontractors.	No Exceptions Noted
	Customer can provide their issues, complaints, or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and Client Contracts and determined that customers have a mechanism to communicate with the company.	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.**		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Management Review Meetings are held every year to discuss the security level, Internal Audit results, Risks, changes, technology trends, occurrence of incidents, and security initiatives.	Selected a sample of Management Review Meetings held and inspected the minutes to determine that these are held on annually.	No Exceptions Noted
	The Management team meets monthly and discusses the business as well as operational issues.	Selected a sample of management meetings held and inspected the minutes to determine that management meetings are held on a periodic basis.	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.**		
	Organization charts are established that depicts authority, reporting lines and responsibilities for management of its information systems. These charts are communicated to employees and are updated as needed	Inspected the organization chart for an understanding of the hierarchy. Enquired with Management to determine that organisation charts are updated periodically.	No Exceptions Noted
	Company has Information security related policies and procedures that describes information security processes, practices and organization.	Inspected IT Policies to determine that these are documented approved.	No Exceptions Noted
	Information Security Policy & Procedures related to HR policies are reviewed and approved by the Management at least annually.	Inspected IT Policies / HR Procedures to determine that changes during the audit period are approved by IT Head	No Exceptions Noted
	The responsibility of managing Information Security is assigned to CISO. Allocation of information security responsibility is documented in Roles and Responsibilities	Inspected Roles and Responsibilities document to determine that Information Security activities are responsibility of CISO.	No Exceptions Noted
CC1.4	**COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.**		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	The company has documented HR Policies and procedures including recruitment, training and exit procedures.	Inspected the HR Policies and procedures to determine that these are documented	No Exceptions Noted
	Job requirements are documented in the job descriptions, and candidates' abilities to meet these requirements are evaluated as part of the hiring and transfer process.	Inspected the HR Policies and a sample of related job description to determined that requirements for each role are documented and are evaluated as part of the hiring process.	No Exceptions Noted
	New employees sign offer letter as their agreement and acceptance of broad terms of employment including a brief description of position and other terms.	Selected a sample of new joiners and inspected the appointment letter to determine that new joiners accept the terms of employment.	No Exceptions Noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings	Inspected Manpower Planning meeting invite to determine that resource planning is reviewed periodically.	No Exceptions Noted
	Background verification checks on candidates for employment or contract work are carried out in accordance with relevant laws and regulations, and are conducted in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	Inspected the completed background verification checks for a sample of employees and contractors hired during the period to determine that background verification checks were completed for each sampled employee or contractor in accordance with relevant laws and regulations and were in proportion to business requirements, the classification of the information to be accessed, and the perceived risks.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Newly hired personnel are provided sufficient training before they assume the responsibilities of their new position	Enquired with HR Head that all new employees undergo induction training.	No Exceptions Noted
	The induction training given by HR includes security training.	Inspected New Hire Induction Training Presentation to ensure that it includes policies on security. Selected a sample of new joiners and inspected the induction attendance/ training records (on GRC Platform) to determine that new joiners undergo information security trainings.	No Exceptions Noted
	An awareness refresher training on information security is provided to all employees on at least annual basis.	Inspected training records for a sample of employees and determined that annual training was completed.	No Exceptions Noted
CC1.5	**COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.**		
	All critical roles that are likely to have external or internal pressures report into the CEO.	Inspected the Organization chart to determine that all critical roles that are likely to have external or internal pressures report into the CEO.	No Exceptions Noted
	Job descriptions are reviewed by entity management on an annual basis as part of performance appraisals.	Inspected updated job descriptions to determine that job descriptions and roles and responsibilities are revised as an when required.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Performance appraisals are performed at least annually.	Inspected HR Process Handbook to determine that Performance appraisals are performed at least annually.	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.**		
	Internal audits are performed, results are communicated, and corrective actions monitored.	Inspected a sample of internal audit reports & the corrective action taken to determine that an effective internal audit process is in place.	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.**		
	System boundaries in terms of logical and physical boundaries are documented. Network diagrams are in place. System Boundaries are shared with the customers when it is required.	Inspected the IT Policies and the network diagram to determine that the Company has defined system boundaries.	No Exceptions Noted
	Customer responsibilities and appropriate system descriptions are provided in client contracts.	Inspected Client contracts for terms related to brief requirements of the system and customer responsibilities	No Exceptions Noted
	Security policies are published on shared directory and GRC Platform.	Inspected the shared directory and GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	An organizational wide incident management process is in place.	Inspected Incident Management Procedures to determine inclusion of documented procedure for identifying incidents.	No Exceptions Noted
	Entity communicates its commitment to security as a top priority for its customers via contracts.	Inspected client contracts of sampled customers to determine entity communicates its commitment to security as a top priority for its customers via contracts.	No Exceptions Noted
	All system changes that affect internal and external users are communicated in a timely manner.	Inspected ISMS and related change management policies to determine how changes to the system are communicated to users.	No Exceptions Noted
	External Client communication is carried out on a timely manner by the Project Manager or Lead using a standard client specific escalation matrix.	Selected a sample of clients and inspected the escalation procedures to determine that these are established.	No Exceptions Noted
	Banners are provided on customer facing applications for communicating changes or downtime such as maintenance window	Enquired with management to determine that only major changes are communicated to clients through banners announcing changes or maintenance windows.	No Exceptions Noted
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. Operations team communicates these changes to the customers.	Enquired with CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions Noted
	New employees hired at senior levels are communicated to stakeholders by HR through Email.	Enquired that senior management hires are communicated internally and if necessary, externally.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
CC2.3	**COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.**		
	Company's security, availability and confidentiality commitments regarding the system are included in the client contracts and service agreements.	Inspected sample of Client SOW, MSA and NDA and determined that terms related to delivery of services are covered.	No Exceptions Noted
	Security policies are published on shared directory & GRC Platform.	Inspected the shared directory & GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted
	The induction training given by HR includes security training.	Inspected New Hire Induction Training Presentation to ensure that it includes policies on security. Selected a sample of new joiners and inspected the induction attendance/ training records (on the GRC Platform) to determine that new joiners undergo information security trainings.	No Exceptions Noted
	Customer responsibilities are described in client contracts.	Inspected a sample of client contracts to determine the explicit responsibilities of customers.	No Exceptions Noted
	Users are informed of the process for reporting complaints and security breaches during induction Security Training.	Selected a sample of new employees and inspected evidence to determine that they attended Security Training during induction.	No Exceptions Noted
	Customer can provide their issues, complaints or feedback through email to Business Heads. Employees can raise their complaints and grievances to HR.	Inspected customer resolution clauses in a sample of customer Statement of Work (SOW) and escalation matrix and determined that customers have a mechanism to communicate with the company.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	A client escalation matrix is in place to ensure that communication channels for external users are available.	Inspected the client escalation mechanism to determine that it is implemented.	No Exceptions Noted
	Customer responsibilities are described in the customer contracts and in system documentation.	Inspected a sample of customer SOW for the roles and responsibilities and determined that roles and responsibilities are clearly defined.	No Exceptions Noted
	CISO is responsible for decisions regarding changes in confidentiality practices and commitments. The operations team communicates these changes to the customers.	Enquired with CISO about procedures to authorize changes in confidentiality commitments and subsequent communication to customers.	No Exceptions Noted
	Changes to system boundaries, and network systems are communicated to clients, if it impact their operations	Enquired with CISO that system boundaries and network systems are communicated to clients if it impacts their operations.	No Exceptions Noted
	Incidents impacting external users are communicated to them through emails along with root cause analysis if required.	Enquired with CISO that Incidents impacting external users are communicated to them through emails along with root cause analysis if required.	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.**		
	Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk. This is part of the Risk Management Framework.	Inspected Risk Assessment and Risk Treatment procedure to determine that Risk Assessment Scales (Risk Rating scales) are defined to evaluate and assess the significance of Risk.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedure to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
	Management evaluates the need for additional resources in order to achieve business objectives as part of its periodic management meetings.	Inspected a sample of Manpower Planning sheet to determine that resource planning is reviewed periodically.	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.**		
	Risk Assessment and Risk Treatment Procedure related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment and Risk Treatment Procedure to determine that the Company has a defined and documented risk assessment process.	No Exceptions Noted
	A risk assessment is performed annually or whenever there are changes in security posture. As part of this process, threats to security are identified and the risk from these threats is formally assessed.	Inspected Risk Assessment and Risk Treatment performed during the audit period to determine updating of asset inventory, threats and risks and to determine that risk assessment is carried out at least on an annual basis.	No Exceptions Noted
	Identified risks are rated and get prioritized based on their likelihood, impact, priority and the existing control measures.	Inspected Risk Assessment performed during the year to determine identified risks are rated	No Exceptions Noted
	All information assets are identified in an asset inventory.	Inspected the Asset Inventory to determine that all information assets are identified in an asset inventory.	No Exceptions Noted
CC3.3	**COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.**		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	The IT department maintains an up-to-date listing of all software and the security patches related to OS and application and patches are applied manually after testing in the QA Environment.	Inspected patching maintenance sheet to determine that patches are applied periodically.	No Exceptions Noted
	List of all hardware is maintained as part of asset register.	Inspected the asset register list to determine that all assets are recorded.	No Exceptions Noted
	Consultadd has defined a formal Risk Assessment and Risk Treatment procedure for evaluating risks based on identified Probability, Impact, Risk Rating, Risk Priority, and mitigating controls.	Inspected Risk Assessment and Risk Treatment procedure to determine that the Consultadd has a defined and documented risk assessment process.	No Exceptions Noted
CC3.4	**COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.**		
	Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	Inspected Non-Disclosure Agreement of sampled vendor to determine that confidentiality commitments, are reviewed by appropriate Entity management during the procurement process.	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.**		
	The internal audit function conducts system security reviews annually by rotating different areas. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	IT system access is reviewed on a quarterly basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are reviewed regularly, and user access lists are reconciled against active HR records.	No Exceptions Noted
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that Vulnerability assessment & penetration tests are carried out periodically and that vulnerabilities were closed.	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.**		
	The internal audit function conducts system security reviews annually by rotating different areas. Results and recommendations for improvement are reported to management.	Inspected a sample of internal audit reports & the corrective action taken to determine that internal audits and system reviews are performed periodically.	No Exceptions Noted
	Company uses a physical firewall, by FortiGate 200F to monitor traffic.	Inspected the FortiGate 200F firewall configuration settings to determine that the IPS/IDS and content filtering.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	IT system access is reviewed on a quarterly basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are reviewed regularly and user access lists are reconciled against active HR records.	No Exceptions Noted
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
	Results of the vulnerabilities and internal external tests are reviewed by the management.	Enquired with CISO that Results of the vulnerabilities and internal external tests are reviewed by the management.	No Exceptions Noted
	All internal audit issues are tracked until closure to ensure that these are closed.	Inspected the Internal Audit results that issues are tracked until closure to ensure that these are closed.	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.**		
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Internal audits including access reviews are performed annually. Results and recommendations for improvement are reported to management.	Inspected sample of annually audit reports to determine that audits are performed periodically.	No Exceptions Noted
	Segregation of duties is in place for critical functions and departments.	Inspected Roles and Responsibilities document to determine that Segregation of duties is in place.	No Exceptions Noted
CC5.2	**COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.**		
	Vulnerability assessment & penetration tests of Network are performed annually by a third party.	Inspected the latest vulnerability assessment /penetration test report performed by third party and determined that VA/PT are carried out periodically and that vulnerabilities were closed.	No Exceptions Noted
	Internal audits including access reviews are performed annually. Results and recommendations for improvement are reported to management.	Inspected annually audit reports (covering different areas) to determine that audits are performed periodically	No Exceptions Noted
	Policies and procedures related to risk management are developed, implemented, and communicated to personnel.	Inspected Risk Assessment & Treatment Procedure to determine that the Company has a defined and documented risk assessment process.	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.**		
	Escalation procedures are defined at relevant places within the policies for policy exceptions.	Inspected client escalation matrix to determine that escalation procedure is in place.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	All policies and procedures clearly define the roles, responsibilities and accountability for executing policies and procedures.	Inspected the job descriptions, roles & responsibilities to determine that these are defined in written job descriptions.	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.**		
	Company has documented procedure for logical access controls.	Inspected the access control policy and procedure and determined that these are documented.	No Exceptions Noted
	Access is granted on least privileges basis as default and any additional access needs to be approved.	Inspected access control procedure document and determined that access is granted on least privileges basis as default and any additional access needs to be approved.	No Exceptions Noted
	Company has established hardening standards infrastructure that include requirements for implementation of firewall, access control, configuration settings, and standardized policies.	Inspected IT policies and procedures to determine that hardening standards have been established.	No Exceptions Noted
	Company does not allow customers or external users to access its systems.	Inspected the evidence and determined that external users cannot access company's network systems	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	The company has Local Windows Authentication. Group Policies are configured via the Local Group Policies for workstation permissions.	Inspected the Local Windows Authentication dashboard and determined that company uses Local Windows Authentication and access provisioning is done based upon the Group Policies. Observed the Group Policies set by the Admin user of Local Windows Authentication.	No Exceptions Noted
	The IT department maintains an up-to-date listing of all software.	Inspected the software list maintained by the IT to ensure that it is up to date. Inspected the software installed in sample desktop to ascertain that current versions are installed.	No Exceptions Noted
	All Assets are assigned owners who are responsible for evaluating access based on job roles. The owners define access rights when assets are acquired or changed.	Inspected the asset register and determined that assets and their owners are clearly documented.	No Exceptions Noted
	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Team Lead and IT Head and reviewed by IT on a periodic basis.	Inspected Local Windows Authentication Group policy and Access Control Matrix to determine that administrator privileges for the domain were limited to IT team and privileged user.	No Exceptions Noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Password policy is set at the Local Policy level. Passwords are manually set on each user desktops by the IT team. The following password parameters are in place: 1. Minimum Length of 8 characters 2. Complexity is enabled.	Inspected the default password security setting in the domain group policy to determine that password settings are: 1. Minimum Length of minimum 8 characters 2. Complexity is enabled	No Exceptions Noted
	Employees don't have access to printers or any other output device. Printer access is given for few teams such as HR and Finance.	Enquired with IT team that no printer access is given to employees and determined based on enquiry that output access is controlled.	No Exceptions Noted
	All confidential data is classified as per the data classification policy.	Inspected information security policies to determine that data classification policies are documented.	No Exceptions Noted
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.**		
	On the day of joining, HR will send a mail to the IT Help desk providing the details of the new joiners. The IT then provides necessary access as per the request. Employee user accounts are removed from various applications and network systems as of the last date of employment manually based on access revocation requests sent by the HR department.	Inspected the Access Control procedure and determined that granting, modifying, or deactivating access is only done against written authorization. Inspected access request forms/emails for a sample of employees to determine that written authorization is in place. Inspected access revocation request /exit checklist for a sample of employees to determine that written authorization for deactivation is in place.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	When an employee leaves the organization, the employee's manager initiates the 'Exit Process'. HR informs respective teams / IT teams within 24 hours to deactivate/delete the user ID from the email system and all applications. An exit checklist is used to ensure compliance with termination procedures.	Selected a sample of exited users and inspected Email from HR to IT and Exit Checklist to determine that the exit process and related account deactivation is as per defined procedures. Inspected Exit IAM to determine that the exited user has disabled status.	No Exceptions Noted
	Privileged access to sensitive resources is restricted to defined user roles and access to these roles must be approved by Team Lead and IT Head and reviewed by IT on a periodic basis.	Inspected Local Windows Authentication's Group Policy to determine that administrator privileges for the domain were limited to IT team and privileged user. Selected a sample of requests for privileged access and Inspected the authorization email to determine that privileged access is authorized by Team Lead and IT Head.	No Exceptions Noted
	Company does not allow non-employees to access its systems.	Enquired with IT staff about access to non-employees.	No Exceptions Noted
	Password policy is set at the Local Policy level. Passwords are manually set on each user desktops by the IT team. The following password parameters are in place: 1. Minimum Length of 8 characters 2. Complexity is enabled.	Inspected the default password security setting in the domain group policy to determine that password settings are: 1. Minimum Length of minimum 8 characters 2. Complexity is enabled	No Exceptions Noted
	Company does not employ contractors in its offices.	Enquired with IT staff about access to non-employees to determine that there are no contractors.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
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.**		
	A role based security process has been defined with in infrastructure based on job requirements.	Inspected the Local Windows Authentication console screens to determine that security centre based on departments and roles have been defined.	No Exceptions Noted
	IT system access is reviewed on a quarterly basis.	Inspected the information security policies containing access controls to determine that these are documented. Inspected Internal Audit Report to determine that access rights are reviewed regularly, and user access lists are reconciled against active HR records.	No Exceptions Noted
	Company does not allow reactivation of ID belonging to an exited employee.	Enquired with IT Head that reactivation of IDs it is prohibited.	No Exceptions Noted
	Account sharing is prohibited unless approved by management.	Inspected Access Control procedure about account sharing and determined that it is prohibited unless authorized in writing. Inspected a system-generated list of user accounts to determine that shared accounts do not exist	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.**		
	Entry to all office premises is restricted to authorized personnel. Physical access control system has been implemented to secure the facilities.	Observed that the entry to premises is restricted by physical security and access control.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Physical access to office premises is monitored through CCTV installed at key points within the premises.	Observed that the CCTV are located at entry exit including the office premises which is working fine.	No Exceptions Noted
	There is a security desk at the office entry manned by a security guard.	Observed the security staff at the reception who ensure that all visitors and employees are screened before entering the office.	No Exceptions Noted
	All visitors have to enter their details in the visitor register.	Inspected the visitor register for a sample of dates to determine that visitor register is maintained.	No Exceptions Noted
	Visitor badges are for identification purposes only and do not permit access to the facility.	Observed that visitor badges are for identification purposes only and do not permit access to any secured areas of the facility.	No Exceptions Noted
	All visitors must be escorted by a Company employee when visiting office facilities.	Observed that all visitors are escorted by a Company employee when visiting Company office.	No Exceptions Noted
	ID cards that include an employee picture must be worn at all times when accessing or leaving the facility.	Observed a sample of employees that employees wear picture IDs at all times.	No Exceptions Noted
	Physical access is setup by the HR Dept for new joiners after all HR formalities are completed. ID cards by default does not have access to any of the sensitive areas.	Selected a sample of new employees and inspected that the access rights were granted in the physical access system only to authorised new joiners.	No Exceptions Noted
	Physical access to sensitive areas/server rooms is granted only to privileged users / IT Team Access to such a restricted zone is given against written request by the CEO.	Inquired with IT Team that access to server room and other sensitive areas is granted only to IT team.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	A periodic review of physical access to sensitive areas against active employee list is carried out by IT.	Inspected a sample of access review reports for sensitive areas to determine that access rights are reviewed regularly.	No Exceptions Noted
	Upon the last day of employment, HR Team sends exit email requesting for deactivation of physical access for terminated employees. Physical access is deactivated by the Admin Team.	Inspected system to determine that the employee ID numbers for the sample of exited employees were deleted from the electronic access control system.	No Exceptions Noted
	Employees are required to complete their exit clearance process on the last day, and all access are disabled.	Inspected the exit checklist for a sample of terminated employees to determine that access is disabled. Inspected the electronic access control system activation / deactivation log to ensure that access of terminated employees have been revoked.	No Exceptions Noted
	On a quarterly basis, Internal audit / HR performs a reconciliation that physical access for terminated employees has In fact been deactivated in the physical access system.	Selected a sample of quarters and inspected physical access reviews to determine that physical access reviews/reconciliations are performed periodically.	No Exceptions Noted
	No contractor is given physical access or electronic access control device.	Enquired with facilities about contractor access and determined no contractor has been given physical access for entering the office.	No Exceptions Noted
	The sharing of access badges and tailgating are prohibited by policy.	Observed that access badges are not shared & no tailgating observed.	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.**		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Media Handling Policy is implemented for procedures relating to the disposal of information assets/equipment.	Inspected Media Handling Policy to determine that procedures relating to disposal of information assets/equipment are implemented.	No Exceptions Noted
	All data is erased from laptops and other media prior to destruction disposal	Enquired with IT Head that all data is erased from laptops and other media prior to destruction disposal. On the employee's last working day, the IT team ensures that all organizational data is securely removed from the laptop before access is revoked.	No Exceptions Noted
CC6.6	**The entity implements logical access security measures to protect against threats from sources outside its system boundaries.**		
	Data is stored in encrypted format, the Disk-level encryption settings are configured for all the end-point devices.	Inspected disk encryption is enabled using default system tools (e.g., BitLocker for Windows, FileVault for macOS) as part of endpoint security checks.	No Exceptions Noted.
	Users access Client system only after logging into company network followed by connecting into client network using encrypted channels such as SSL/VPN.	Inspected evidence for connecting with client's environment via SSL/VPN connection.	No Exceptions Noted
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.**		
	Entity policies prohibit the transmission of sensitive information over the Internet or Other public communications paths unless it is encrypted.	Inspected the information security policies to determine that transmission of sensitive information over the internet happens only when the information is encrypted.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	External users access applications hosted at cloud infrastructure through secure https with SSL/TLS certificates.	Inspected evidence for implementation of HTTPS encryption to determine that secure HTTPS connections are used.	No Exceptions Noted
	Use of removable media is prohibited by policy except when authorized by management.	The review determined that removable media access was not disabled for laptops, and desktops in accordance with policy, which prohibits its use except when explicitly authorized by management.	Exception Noted: Removable media access was not disabled on laptops, and desktops. **Management Response:** Consultadd accepts USB access as a risk and plans to implement an MDM solution to manage all devices before the next audit.
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.**		
	Antivirus software is installed on workstations, laptops, and servers. This system provides antivirus system scans and endpoint protection.	Inspected a sample of Laptops and determined that antivirus is installed, and signature files were updated.	No Exceptions Noted
	The ability to install software on workstations and laptops is restricted to IT support personnel through admin accounts.	Inspected the Information Security Policies to determine that users are not allowed to install any software.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Any viruses discovered are reported to the IT team either by the antivirus system or by the affected employees.	Inspected the antivirus console for configuration details about updating and alerts.Inspected the security training pack for the instructions to employees about virus incidence reporting.	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.**		
	Management has defined configuration standards and hardening standards.	Inspected System Hardening Policy to determine that Management has defined configuration standards and hardening standards.	No Exceptions Noted
	The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Inspected monthly reports from the IT department that summarise non-compliance with standards to determine that Infrastructure and software non-compliances are tracked and reported.	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.**		
	Hardening Checklists are in place for hardening of IT infrastructure/desktops.	Inspected the System Hardening Checklist to determine that Management has defined configuration standards and hardening standards.	No Exceptions Noted
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.**		

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	A formal, defined incident management Policy is documented as part of Information Security Policies for evaluating reported events.	Inspected Incident Management Policy to determine that incident management process is documented.	No Exceptions Noted
	Incidents are reported to the IT team by phone or email. These are tracked through Incident log on Excel.	Inspected the screenshot of the incident log to determine that incidents are tracked.	No Exceptions Noted
	Reported incidents are logged in Excel/Incident form and include the following details Incident Type Data and Time of incident Details Action Taken Root Cause (For select high risk incidents)	Inspected a sample of incident report to determine that incidents covered Incident Type, Data and Time of incident, Details, Action Taken, Root Cause as per defined process.	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.**		
	All security incidents are also reviewed and monitored by the Information Security Group. Corrective and preventive actions are completed for incidents.	Inspected minutes of ISG committee meeting minutes to determine that discussion on incidents takes place.	No Exceptions Noted
	Change management requests are opened for events that require permanent fixes.	Inspected Incident Management Procedure and determined that for some incidents, change requests are opened as part of the resolution.	No Exceptions Noted
	All incidents are evaluated and necessary action taken to close the threat/vulnerability	Inspected Incident Management Procedure and determined that necessary action is taken to close the threat/vulnerability.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Inspected Incident Management Procedure and determined that necessary action is taken for communicating security incidents and actions taken to affected parties are developed and implemented	No Exceptions Noted
	Management reviews all incidents that occurred during the year is conducted and headed by CISO.	Inspected MRM Meeting minutes to determine that annually management reviews all incidents that occurred during the year is conducted.	No Exceptions Noted
	HR policies include a code of conduct and disciplinary policy for employee misconduct.	Inspected the HR Policies for Code of Conduct and Disciplinary Policy.	No Exceptions Noted
CC7.5	**The entity identifies, develops, and implements activities to recover from identified security incidents.**		
	All incidents are evaluated and necessary action is taken to close the threat/vulnerability.	Inspected Incident Management Procedure and determined that necessary action is taken to close the threat/vulnerability.	No Exceptions Noted
	Root cause analysis is performed for major incidents.	Inspected the screenshot of the incident log and related root cause description for some incidents to determine that incidents are tracked.	No Exceptions Noted
Change Management			
CC8.1	**The entity authorizes, designs, develops acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.**		
	Changes are communicated to the appropriate client and user community if the change has any potential impact on the user base.	Enquired with IT Head that changes are communicated to clients and end users if it has an impact on those users.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	The change management policy has defined roles and assignments thereby providing segregation of roles in the change management process.	Inspected the Change Management Policy and Procedures to determine that these define the segregation of roles for change management.	No Exceptions Noted
	Entity has defined its change management and approval processes in its information security policies.	Inspected Information Security Policy and determined that change management policy and procedures are defined.	No Exceptions Noted
	All change requests are logged and change request ticket created.	Selected a sample of change requests to determine that these are logged and that changes are approved by IT Head.	No Exceptions Noted
	A risk assessment is performed on a periodic basis. The risk assessment includes identifying potential threats and assessing the risks associated with identified. Change requests are created based on the identified needs.	Inspected the risk management procedures to determine if change requests are created based on identified needs.	No Exceptions Noted
Risk Mitigation			
CC9.1	**The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.**		
	Entity has a documented Business Continuity Procedure & Plan including Disaster Recovery guidelines to be used in the event of an event necessitating systems infrastructure recovery.	Inspected the Business Continuity Procedure & Plan to determine that a plan and procedure have been documented with clear responsibilities on those required to respond.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Business continuity and disaster recovery plans, including restoration of backups, are tested annually.	Inspected the Business Continuity Planning Policy and determined that BCP plans are tested annually. Inspected the BCP Test Report to determine that BCP testing was carried out during the audit period.	No Exceptions Noted
CC9.2	**The entity assesses and manages risks associated with vendors and business partners.**		
	New Third-Party Service Providers are selected based on a Vendor Selection Process. Security risk assessment is a key part of the vendor selection process. Company requires all key subservices to be compliant with security certifications and attestations such as ISO 27001, SOC1 or SOC2.	Enquired with Management that vendors and third-party service providers are selected based on a vendor due diligence. Enquired with Management that there was no material third party vendor that was onboarded during the audit period.	No Exceptions Noted
	Periodic monitoring of third-party vendors is performed that include regular conversations and issue management	Inspected Vendor Management Module to confirm periodic monitoring of third-party vendors is in place.	No Exceptions Noted
	A formal contract is executed between Company and Third-Party Service Providers before the work is initiated. Agreement includes terms on confidentiality, responsibilities of both parties.	Inspected a sample of vendor contracts to determine that vendors contracts are in place. Enquired with Facilities Head that there are no new vendors that are onboarded during the current period.	No Exceptions Noted
	All customer & vendor contracts have terms related to confidentiality.	Inspected an NDA and vendor contracts to determine that it contains clauses relating to confidentiality.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	A confidentiality agreement is signed by all employees at the time of joining. In addition, NDAs are signed with third parties wherever required.	Inspected the confidentiality agreement template to determine that agreements include terms on confidentiality and non-disclosure.	No Exceptions Noted
ADDITIONAL CRITERIA FOR AVAILABILITY			
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.**		
	The Entity monitors system processing capacity and usage and takes correction actions to address changing requirements. Processing capacity of systems including FortiGate 200F physical firewall and Physical server component is monitored Manually on an ongoing basis.	Inspected a sample of capacity monitoring reports to verify that the capacity demand is documented and reviewed by management.	No Exceptions Noted
	Critical infrastructure components including FortiGate 200F physical firewall, ISP, Physical servers have been reviewed for criticality classification and assignment of a minimum level of redundancy.	Inspected redundancy measures for ISP and determined that there is a backup ISP available and maintained by office service provider.	No Exceptions Noted.
A1.2	**The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup, and recovery infrastructure to meet its objectives.**		
	Environmental controls (fire extinguishers, fire sprinklers and smoke detectors) have been installed to protect perimeter area. CCTV are installed at key points for surveillance. Devices are checked on a periodic basis and checklists are prepared.	Observed that fire extinguisher across all office premises that these are in working condition. Observed other environmental controls.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Fire drill is conducted annually.	Observed the fire drill report and verified that there were no exceptions noted.	No Exceptions Noted
	Uninterruptible power supply (UPS) devices are in place to secure critical IT equipment against power failures and fluctuations. (DG set of sufficient capacity is provided to provide power during outage as part of lease by building owner)	Observed the UPS installed at the premises to determine that they are in good working condition.	No Exceptions Noted
	Company has multiple ISPs in place to provide redundancy in case of link failure	Inspected the network diagram to determine that the company has multiple ISPs in place.	No Exceptions Noted
	Vendor warranty specifications are complied with and tested to determine if the system is properly configured.	Inspected MSAs, building lease and vendor contract for maintenance of various environmental controls.	No Exceptions Noted
	Facilities and admin personnel monitor the status of environmental protections on a regular basis. Maintenance checklists are used where applicable.	Inspected environmental control check report and determined that maintenance reviews are carried out. Inspected the UPS preventive maintenance reports, vendor maintenance contracts to determine that preventive maintenance is performed periodically.	No Exceptions Noted
	Backup policy is defined in the information security policies.	Inspected information security policies to determine that backup schedules, frequency of backups are documented.	No Exceptions Noted
A1.3	**The entity tests recovery plan procedures supporting system recovery to meet its objectives.**		
	Business Continuity Plan and Procedure including Disaster recovery for various disruption scenarios are documented.	Inspected Business Continuity Plan and Procedure to determine that these are documented.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Business continuity plans, are tested on annual basis.	Inspected BCP/DR test report to determine that BCP plans have been tested.	No Exceptions Noted
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1	**The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.**		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the Data Protection and Security policy to determine that the Company retains information as per the defined policies.	No Exceptions Noted
C1.2	**The entity disposes of confidential information to meet the entity's objectives related to confidentiality.**		
	The entity establishes written policies related to retention periods for the confidential information it maintains. The entity securely destroys or deletes all data as soon as it is no longer needed.	Inspected the Data Protection and Security policy to determine that the Company destroys or disposes of confidential information as per the defined retention policies.	No Exceptions Noted
	Security policies are published on shared directory and GRC Platform.	Inspected the shared directory and GRC Platform to determine that IT security policies available to internal users.	No Exceptions Noted
C 1.2 A	**Client Contracts**		
	Processing is scheduled and performed appropriately in accordance with client specifications, instructions and delivery priority; deviations from the schedule are identified and resolved in a timely manner.	Selected a sample of clients and inspected the client contracts to determine that service provisioning is based on client contracts.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	Processing is performed appropriately in accordance with client SLAs.	Selected a sample of clients and inspected the SLA terms to determine that SLA terms are complied with Escalation Matrix.	No Exceptions Noted
	Consultadd sends an email to clients to setup the user credentials. Clients setup user credentials and then email them back to the company.	Inspected the screenshots to determine that at Consultadd the client entity shared the official e-mail IDs using which Consultadd Employees would access the client's environment. Inspected a sample of clients to determine communication to create Email ID is present.	No Exceptions Noted
	On exit of the employees, clients are notified of the exit so that the user credentials can be disabled.	Inspected the screenshots of notification to the client about access revocation to resources. E-mail for unavailability of resources and new resource allocation to client project was also evidenced.	No Exceptions Noted
C 1.2 B	**Output Deliverables and Quality Assurance**		
	Files are reviewed and/or a quality check is performed to ensure work is as per client specification.	Enquired that bi-weekly client project quality checks are performed, this was verified as mentioned in the Kick-off sheet.	No Exceptions Noted
C 1.2 C	**Client Reporting**		
	A Weekly / monthly status report is used to keep track of all support requests coming in from customers. Management reviews activities on weekly / monthly basis. Periodic reporting to clients is carried out. Informal calls, and email updates are regularly carried out.	Selected a sample and inspected the monthly status reports to determine that monthly reporting are carried out with clients as part of client operations.	No Exceptions Noted

Control #	Control Activity Specified by the Service Organization	Test Procedures Applied by the Service Auditor	Test Results
	The Company has developed a client onboarding checklist for its new client setup and transition process and post-go-live operations processes.	Inspected the client onboarding checklist to determine that these are documented.	No Exceptions Noted

SECTION 5

OTHER INFORMATION PROVIDED BY CONSULTADD

Other Information Provided by Consultadd

The information provided in this section is provided for informational purposes only by Consultadd. Independent Auditor has performed no audit procedures in this section.

Disaster and Recovery Services

The AICPA has published guidance indicating that business continuity planning, which includes disaster recovery, is a concept that addresses how an organization mitigates future risks as opposed to actual controls that provide user auditors with a level of comfort surrounding the processing of transactions.

In addition to the physical Consultadd has implemented logical controls to safeguard against interruption of Consultadd has developed a number of procedures that provide for the continuity of operations in the event of an availability zone failure by spinning up multiple servers across all availability zones.

The disaster recovery plan defines the roles and responsibilities and identifies the critical IT application programs, operating systems, personnel, data files, and time frames needed to ensure high availability and system reliability based on a business impact analysis.

CERTIFICATE *of* SIGNATURE

REF. NUMBER
CAEMZ-U5ZDL-EWVPE-TEMNN

DOCUMENT COMPLETED BY ALL PARTIES ON
17 JUL 2025 17:42:15 UTC

SIGNER	TIMESTAMP	SIGNATURE
ANKIT PATHAK EMAIL ANKIT.P@CONSULTADD.COM	SENT 17 JUL 2025 05:19:27 UTC VIEWED 17 JUL 2025 17:41:40 UTC SIGNED 17 JUL 2025 17:42:15 UTC	 IP ADDRESS 108.53.76.205 LOCATION JERSEY CITY, UNITED STATES

RECIPIENT VERIFICATION

EMAIL VERIFIED
17 JUL 2025 17:41:40 UTC

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
Info Technology

Proc Folder:	2028979
Doc Description:	Addendum No 1-Advanced Email Security
Proc Type:	Central Master Agreement
Reason for Modification:	Addendum No 1 is issued to publish vendor questions with agency responses and to modify the bid opening date.

Date Issued	Solicitation Closes	Solicitation No	Version
2026-08-18	2026-08-25 13:30	CRFQ 0231 OOT2700000005	2

BID RECEIVING LOCATION

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

VENDOR

Vendor Customer Code:

Vendor Name : Consultadd Inc.

Address : WTC 3

Street : 175 Greenwich Street, 38th Floor

City : New York

State : NY **Country :** US **Zip :** 10007

Principal Contact : Bharat Bhate, Founder and President

Vendor Contact Phone: (888) 771 9958 **Extension:**

FOR INFORMATION CONTACT THE BUYER
Toby L Welch
(304) 558-8802
toby.l.welch@wv.gov

Vendor Signature X  **FEIN#** 274565433 **DATE** 08/24/2026

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 publish vendor questions with the agency's responses. 2) To modify the bid opening date from 8/19/26 to 8/25/26 ---no other changes---

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
1	Core Detection	22000.00000	EA	$3.7	$81,400

Comm Code	Manufacturer	Specification	Model #
43230000	Check Point Software Technologies	Advanced Email Security	CPI INF BAS C100

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO		SHIP TO	
DEPARTMENT OF ADMINISTRATION		WV OFFICE OF TECHNOLOGY	
OFFICE OF TECHNOLOGY		BLDG 5, 10TH FLOOR	
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR		1900 KANAWHA BLVD E	
CHARLESTON	WV	CHARLESTON	WV
US		US	

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
2	Core Detection - Year 2 (Optional Renewal)	22000.00000	EA	$3.7	$81,400

Comm Code	Manufacturer	Specification	Model #
43230000	Check Point Software Technologies	Advanced Email Security	CPI INF BAS C100

Extended Description:
Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
3	Core Detection - Year 3 (Optional Renewal)	22000.00000	EA	$3.9	$85,800

Comm Code	Manufacturer	Specification	Model #
43230000	Check Point Software Technologies	Advanced Email Security	CPI INF BAS C100

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

INVOICE TO	SHIP TO
DEPARTMENT OF ADMINISTRATION	WV OFFICE OF TECHNOLOGY
OFFICE OF TECHNOLOGY	BLDG 5, 10TH FLOOR
1900 KANAWHA BLVD E, BLDG 5 10TH FLOOR	1900 KANAWHA BLVD E
CHARLESTON WV	CHARLESTON WV
US	US

Line	Comm Ln Desc	Qty	Unit Issue	Unit Price	Total Price
4	Core Detection - Year 4 (Optional Renewal)	22000.00000	EA	$3.9	$85,800

Comm Code	Manufacturer	Specification	Model #
43230000	Check Point Software Technologies	Advanced Email Security	CPI INF BAS C100

Extended Description:

Core Detection per Mailbox estimated 22,000 Mailboxes
The usage amount provided is an estimate only. Actual usage may be higher or lower, and the figure is not guaranteed.

SCHEDULE OF EVENTS

Line	Event	Event Date
1	Questions are due by 3:00 p.m.	2026-08-11

	Document Phase	Document Description	Page 4
OOT2700000005	Final	Addendum No 1-Advanced Email Security	

ADDITIONAL TERMS AND CONDITIONS

See attached document(s) for additional Terms and Conditions

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: CRFQ OOT27*005

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)

[X]	Addendum No. 1	[ ]	Addendum No. 6
[ ]	Addendum No. 2	[ ]	Addendum No. 7
[ ]	Addendum No. 3	[ ]	Addendum No. 8
[ ]	Addendum No. 4	[ ]	Addendum No. 9
[ ]	Addendum No. 5	[ ]	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.

Consultadd Inc.
Company

Authorized Signature

08/24/2026
Date

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

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.

(Printed Name and Title) Bharat Bhate, Founder and President

(Address) WTC 3, 175 Greenwich Street, 38th Floor, New York, NY 10007

(Phone Number) / (Fax Number) (888) 771 9958

(email address) publicservices@consultadd.com

CERTIFICATION AND SIGNATURE: By signing below, or submitting documentation through *wv*OASIS, 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 this bid or offer was made without prior understanding, agreement, or connection with any entity submitting a bid or offer for the same material, supplies, equipment or services; that this bid or offer is in all respects fair and without collusion or fraud; that this Contract is accepted or entered into without any prior understanding, agreement, or connection to any other entity that could be considered a violation of law; 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.

Consultadd Inc.
(Company)

(Signature of Authorized Representative)

Bharat Bhate, Founder and President
(Printed Name and Title of Authorized Representative) (Date)

(888) 771 9958 08/24/2026
(Phone Number) (Fax Number)

publicservices@consultadd.com
(Email Address)

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.

11.0 MISCELLANEOUS:

11.1 No Substitutions: Vendor shall supply only Contract Items submitted in response to the Solicitation unless a contract modification is approved in accordance with the provisions contained in this Contract.

11.2 Vendor Supply: Vendor must carry sufficient inventory of the Contract Items being offered to fulfill its obligations under this Contract. By signing its bid, Vendor certifies that it can supply the Contract Items contained in its bid response.

11.3 Reports: Vendor shall provide quarterly reports and annual summaries to the Agency showing the Agency's items purchased, quantities of items purchased, and total dollar value of the items purchased. Vendor shall also provide reports, upon request, showing the items purchased during the term of this Contract, the quantity purchased for each of those items, and the total value of purchases for each of those items. Failure to supply such reports may be grounds for cancellation of this Contract.

11.4 Contract Manager: During its performance of this Contract, Vendor must designate and maintain a primary contract manager responsible for overseeing Vendor's responsibilities under this Contract. The Contract manager must be available during normal business hours to address any customer service or other issues related to this Contract. Vendor should list its Contract manager and his or her contact information below.

Contract Manager: Bharat Bhate
Telephone Number: (888) 771 9958
Fax Number: N/A
Email Address: publicservices@consultadd.com

AGREED:

Name of Agency:_____	Name of Vendor: Consultadd Inc.
Signature:_____	Signature: 
Title:_____	Title: Founder and President
Date:_____	Date: 08/24/2026

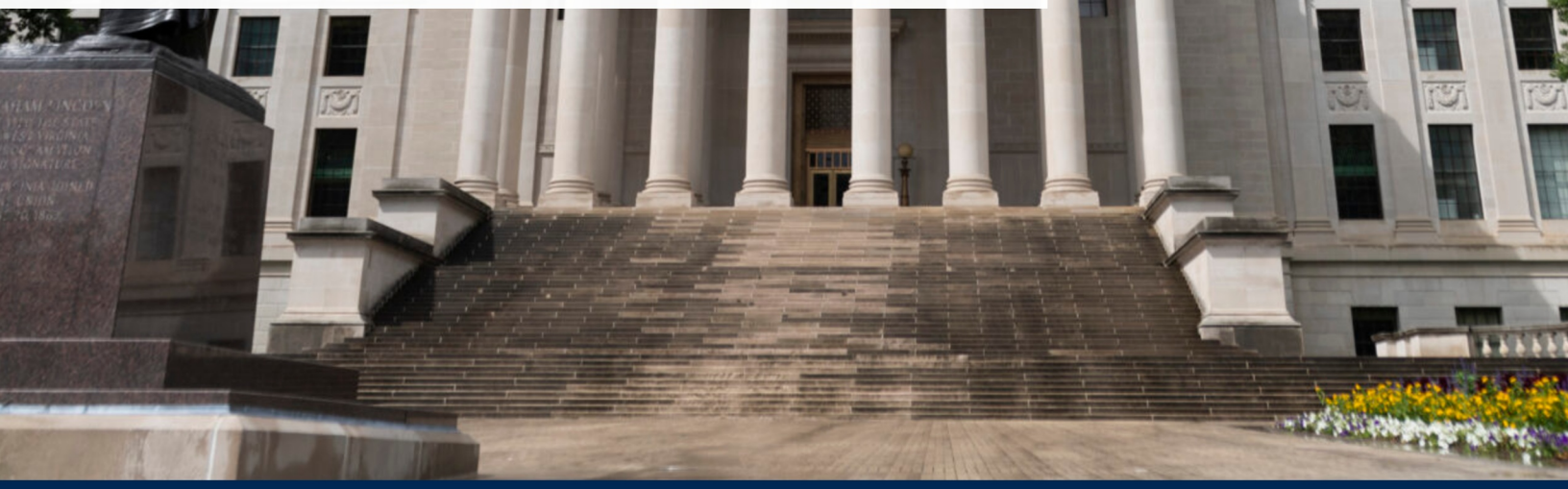
consultadd Public Services

Proposal for:

Advanced Email Security

CRFQ-0231-OOT2700000005

State of West Virginia



Contact No.
+1 888 771 9958

Email Address
publicservices@consultadd.com

Website:
consultaddpublicservices.com

HQ Address
175 Greenwich Street, 38th Floor, New York, NY, 10007

TABLE OF CONTENTS

COVER LETTER

August 25, 2026

Toby L. Welch
State of West Virginia
Department of Administration, Purchasing Division
2019 Washington Street East
Charleston, WV 25305

Re: CRFQ 0231 OOT2700000005 - Advanced Email Security

Dear Mr. Welch,

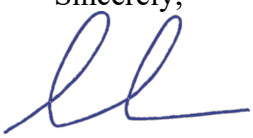
Consultadd Public Services (division of Consultadd Inc) is pleased to submit its response to the State of West Virginia's request for Advanced Email Security services on behalf of the West Virginia Office of Technology.

We understand the State's objective is to strengthen protection for its Google Workspace environment by adding an advanced email security layer focused on phishing, business email compromise, and related email-based threats. We also recognize the importance of doing so in a way that supports the State's existing operations, avoids unnecessary disruption, and provides a scalable solution for approximately 22,000 mailboxes.

Our response is structured to support the State's priorities for security, operational continuity, compliance, and clear pricing. The proposed solution is intended to help WVOT improve threat detection and prevention while preserving the native Google Workspace mail flow and minimizing impact on end users.

Consultadd acknowledges Addendum No. 1 and confirms that the agency responses and revised closing date have been incorporated into this submission. Consultadd appreciates the opportunity to support the State of West Virginia in this important cybersecurity initiative. We look forward to the possibility of serving WVOT and contributing to a secure, reliable, and well-supported email environment for the State.

Sincerely,



Bharat Bhate
Founder & President
Consultadd Inc.
Email: publicservices@consultadd.com
Phone: (888)-771-9958

ABOUT CONSULTADD PUBLIC SERVICES

Founded in 2011 and headquartered in New York City, New York, Consultadd is an information technology services and consulting firm supporting public-sector and commercial organizations with secure, scalable, and outcome-focused technology solutions. Through Consultadd Public Services, the company provides dedicated support to federal, state, local, education, and public-purpose organizations across the United States.

Consultadd brings experience across cybersecurity, cloud services, managed services, application modernization, implementation and integration, licensing support, staff augmentation, and technology advisory services. This range of capabilities allows Consultadd to support agencies not only with technology procurement, but also with the planning, coordination, implementation, and support activities needed to help solutions succeed in operational environments. Consultadd's delivery approach is built around security, responsiveness, and public-sector accountability. The company maintains a mature compliance and security posture supported by credentials and practices including ISO 27001, SOC 2 Type II, CMMC alignment/readiness, HIPAA compliance, and FERPA compliance. Consultadd is also a GSA-approved contract holder and CMAS contract holder, supporting streamlined access to technology services for eligible public-sector customers.

With experience serving more than 200 clients across commercial and public-sector environments, including Fortune 500 organizations and federal agencies, Consultadd understands the importance of reliable service delivery, secure implementation, and clear communication. The company is registered in 44 states and maintains a distributed delivery model, enabling access to skilled resources across the country and supporting onsite assistance when required by the agency. For the West Virginia Office of Technology, Consultadd will bring a practical, agency-focused approach centered on secure solution delivery, vendor coordination, clear escalation paths, and minimal disruption to existing operations. The goal is to support WVOT with an advanced email security solution that aligns with the State's Google Workspace environment, security priorities, and operational continuity needs.

Our Credentials

Consultadd in Numbers

200+
Projects Completed Across USA

60+
Government Clients across IT Modernization, Cybersecurity, Cloud Services, Infrastructure Support, and Data-driven Transformation

600+
IT Professionals

40+
Industry Partnership Networks

OUR UNDERSTANDING OF THE PROJECT SCOPE

The West Virginia Office of Technology is seeking an advanced email security solution that strengthens protection across the State's existing Google Workspace environment. The State's stated objective is to detect and prevent phishing attacks, business email compromise, and related email-based threats that may bypass native security controls. The requested solution must support approximately 22,000 mailboxes through a core detection capability priced on a per-mailbox basis.

Consultadd understands that WVOT's priority is not simply to add another security tool, but to implement an email protection layer that works cleanly with the State's existing environment. The solution must preserve native Google Workspace operations while improving the State's ability to identify, prevent, and respond to modern email-based attacks. This includes protection against phishing, business email compromise, malware, malicious links, suspicious sender behavior, account-compromise indicators, and related threats targeting State users.

The State's desired architecture is cloud-based and non-disruptive. The solution must operate through native integration with Google Workspace and must not require changes to MX records, rerouting of email traffic through a third-party gateway, use of an external mail relay, or deployment of on-premises appliances. Consultadd understands this requirement as critical to reducing implementation risk, preserving business continuity, and avoiding unnecessary changes to the State's existing email flow.

The project scope also includes rapid onboarding and activation across the mailbox environment. WVOT requires the vendor to confirm that onboarding and full-mailbox API verification can be achieved within the required timeframe without disrupting active State communications. Consultadd understands this as a key operational requirement and will align the proposed approach around fast activation, clear coordination with State technical stakeholders, and validation that mailbox protection is active across the required environment.

The proposed solution must also support the State's compliance and data-security expectations. WVOT requires confirmation of the applicable compliance pathway and supporting documentation, such as FedRAMP, StateRAMP, or SOC 2 Type II documentation, as applicable to the proposed platform. The response must also address U.S. data residency and demonstrate that the proposed solution can meet the State's requirements for secure processing, storage, and protection of State data.

Consultadd further understands that the State is seeking a clear annual SaaS pricing structure. The CRFQ includes pricing for the base year and optional renewal years for the same estimated mailbox quantity. The proposed pricing must therefore be structured around annual per-mailbox core detection pricing and should include the product updates, support, and core automation capabilities required for the proposed email security service.

Based on this understanding, Consultadd's response is focused on providing WVOT with a practical, secure, and scalable advanced email security solution that can be deployed over the existing Google Workspace environment with minimal operational disruption, clear pricing, and the required vendor-supported security and compliance documentation.

PROPOSED SOLUTION OVERVIEW

Consultadd proposes Check Point Advanced Protect for Google Workspace as the advanced email security solution for the West Virginia Office of Technology's Google Workspace environment. The proposed solution is aligned to the CRFQ line item for Core Detection per Mailbox and is intended to provide advanced detection and prevention capabilities for approximately 22,000 mailboxes.

Field	Proposed Response
Manufacturer	Check Point Software Technologies
Solution Name	Check Point Advanced Protect for Google Workspace
Specification / Description	Advanced Email Security / Core Detection per Mailbox
SKU / Model	CPI-INF-BAS-C100
Target Environment	Google Workspace
Estimated Quantity	Approximately 22,000 mailboxes
Pricing Basis	Annual per-mailbox SaaS subscription pricing
Primary Use Case	Detection and prevention of phishing, business email compromise, and related email-based threats

The proposed solution is intended to serve as an advanced email security layer over the State's existing Google Workspace environment. The CRFQ identifies WVOT's primary objective as the detection and prevention of phishing attacks, business email compromise, and related email-based threats that bypass native security controls. The CRFQ also identifies the applicable pricing item as Core Detection per Mailbox for an estimated 22,000 mailboxes.

Consultadd's proposal is based on the Advanced Protect licensing option. Separate add-on modules for Data Loss Prevention and user-facing email encryption are not included in the proposed base pricing unless later requested by the State as an optional enhancement or change order. Platform-level data protection, encryption in transit and at rest, and applicable SaaS security controls are included as part of the proposed solution.

TECHNICAL RESPONSE TO SCOPE REQUIREMENTS

1. PURPOSE AND SCOPE ALIGNMENT

The West Virginia Office of Technology is seeking an advanced email security solution layered on top of the State's existing Google Workspace environment. The State's stated objective is to detect and prevent phishing attacks, business email compromise, and related email-based threats that may bypass native security controls. The CRFQ identifies the required item as Core Detection per Mailbox for an estimated 22,000 mailboxes, with the usage quantity identified as an estimate that may be higher or lower.

Consultadd's proposed solution is Check Point Advanced Protect for Google Workspace, SKU CPI-INF-BAS-C100, configured to provide advanced email threat detection and prevention across the State's Google Workspace mailboxes. The proposed solution is intended to strengthen WVOT's protection against modern email-based threats while preserving the State's existing email operations and user experience.

The proposed approach is aligned to the State's need for a cloud-based security layer that can operate over the existing Google Workspace environment without requiring a disruptive redesign of the State's email architecture. The solution will provide mailbox-level protection, detection, and response capabilities focused on the threat types identified in the CRFQ, including phishing, business email compromise, malware, malicious links, suspicious sender behavior, and related email-based attacks.

2. GOOGLE WORKSPACE API-BASED ARCHITECTURE

The proposed solution is designed for deployment with Google Workspace through an API-based integration model. Under this model, email traffic continues to flow natively into Google Workspace, and the security platform connects to the environment using authorized Google Workspace APIs to inspect, analyze, and remediate threats.

This architecture supports the State's requirement for a non-gateway deployment model. The proposed solution does not require rerouting email traffic through an external secure email gateway, third-party mail relay, intermediary cloud proxy, or separate appliance. It also does not require MX record changes for the State's email domain. This helps WVOT preserve its existing Google Workspace mail flow while adding an advanced email security layer for threat detection and prevention.

The API-based approach is intended to reduce deployment risk, simplify onboarding, and avoid unnecessary disruption to active State communications. It also supports fast activation across a large mailbox environment because the solution can be authorized and configured through Google Workspace administrative permissions rather than through mail-routing

changes. Because the solution operates through API-based inspection rather than mail-flow routing, Google Workspace email delivery continues natively and does not depend on the scanning layer as a mail-routing dependency or single point of failure.

3. THREAT PROTECTION CAPABILITIES

Check Point Advanced Protect for Google Workspace is proposed as the State's core detection solution for advanced email security. The solution supports protection across inbound, outbound, and internal/east-west email activity, including malicious emails that originate externally, move laterally within the Google Workspace environment, or affect account-based communications after initial compromise.

Capability Area	Proposed Coverage
Phishing Protection	Detection and prevention of phishing attempts, credential-harvesting campaigns, malicious links, suspicious sender behavior, and related email-based threats.
Business Email Compromise Protection	Detection of impersonation, spoofing, social-engineering patterns, executive fraud indicators, vendor invoice fraud patterns, and other BEC-related indicators.
Malware and Attachment Protection	Deep inspection of malicious attachments and payloads using advanced detection controls, including cloud-based sandboxing and dynamic detonation for suspicious files.
URL and Link Protection	The proposed solution supports time-of-click URL inspection and malicious link analysis through its Google Workspace security capabilities, while preserving the State's non-gateway architecture and native mail-flow requirements. The solution is proposed to operate without MX record changes, gateway routing, mail relay routing, cloud proxy routing, or on-premises appliance deployment.
Account Takeover Protection	Detection of anomalous mailbox behavior, compromised-account indicators, suspicious login or mailbox activity, and unauthorized activity patterns.
Internal Email Threat Detection	Detection of threats that may originate from or move laterally within the Google Workspace environment, including internal user-to-user email activity.
Post-Delivery Remediation	Near-real-time quarantine, removal, or remediation of malicious messages identified after delivery, based on configured policies and platform capabilities.
Historical Mailbox Analysis	Retrospective scanning of available mailbox content within the State's Google Workspace retention period, including the required prior 90-day historical dataset for onboarding and evaluation purposes.
Groups and Automated Destinations	Protection for user mailboxes and email flows involving groups, automated destinations, ticketing systems, CRM platforms, forwarded recipients, shared mailboxes, delegated mailboxes, resource mailboxes, and service-account mailboxes included within the State's mailbox population.
Prompt Injection	Detection of email-delivered threats that may target downstream

and AI-Targeted Email Threats	systems, including hidden payloads, malicious instructions, and prompt-injection style content intended to influence AI assistants, copilots, automated workflows, or related systems.
SIEM/SOAR Event Export	Support for threat event export using standard integration methods, including API-based delivery and structured event formats. Consultadd will coordinate with WVOT after award to align the final event-export and SIEM/SOAR integration pattern with the State's identified platforms.
Native Remediation Automation	Automated remediation using native platform workflows without requiring an external XSOAR platform for core malicious-email remediation actions.
Administrative Controls	Role-based access control, delegated administration, agency-level separation, and audit logging of administrative activity to support WVOT's operational and governance requirements.
Google Workspace and Gemini Coexistence	Coexistence with Google Workspace features, including Gemini and related Workspace functions, without disrupting native message rendering, contextual lookups, AI-generated summaries, smart replies, or other Google Workspace user experiences.
Microsoft 365 Future Flexibility	Native support for Microsoft 365 protection for future flexibility while maintaining Google Workspace as the State's current deployment environment.
Palo Alto NGFW Compatibility	Because the proposed solution is API-integrated and does not route, proxy, or inspect network traffic, it does not require changes to the State's Palo Alto Next-Generation Firewall environment and does not introduce architectural conflicts with the State's existing Palo Alto infrastructure.

The proposed solution is focused on the State's requirement for a complete email security platform that detects malicious emails in either direction, supports near-real-time post-delivery remediation, and preserves the State's native Google Workspace mail flow.

4. ARCHITECTURE VERIFICATION STATEMENT

Consultadd's proposed architecture for WVOT is based on a direct cloud-to-cloud integration between Check Point Advanced Protect and the State's Google Workspace environment.

Proposed Architecture Flow

1. State email traffic continues to flow natively into Google Workspace.
2. Check Point Advanced Protect connects to Google Workspace through authorized APIs.
3. The solution analyzes messages, links, attachments, sender behavior, and threat indicators.
4. Suspicious or malicious items are flagged, quarantined, removed, or remediated based on configured policies.
5. Security events and reporting are made available through the solution's administrative console and applicable integration capabilities.

6. WVOT retains the existing Google Workspace mail flow without MX record changes, mail relay routing, gateway proxying, or appliance deployment.

Architecture Verification Statement:

The proposed solution will operate as an API-based advanced email security layer for Google Workspace. Email traffic will continue to flow natively into Google Workspace and will not be routed through an intermediary MX-record route, third-party secure email gateway, external mail relay, or gateway proxy. No on-premises appliance is required for the proposed deployment. The proposed architecture is designed to preserve native Google Workspace mail flow and avoid introducing mail-routing dependencies, including intermediary MX routing, secure email gateway routing, mail relay routing, or gateway proxying.

This architecture is intended to support WVOT's operational continuity, reduce cutover risk, and provide advanced detection and remediation capabilities without changing the State's existing email delivery path.

5. U.S. DATA RESIDENCY STATEMENT

The proposed Check Point Advanced Protect for Google Workspace solution supports U.S. data residency for the State's deployment. All customer data associated with the proposed solution will be stored and processed within the United States.

The solution provides data storage, processing, and protection in accordance with its U.S. data residency controls and is configured to support the State's requirement for secure handling of customer data within the United States.

6. COMPLIANCE VERIFICATION

The proposed Check Point Advanced Protect for Google Workspace solution satisfies the RFP's compliance verification requirement through the SOC 2 Type II pathway. Check Point's official SOC 2 Type II compliance page identifies Email Security under its covered Workspace Security products and states that the applicable controls for listed Check Point products operated effectively during the audit period to meet the relevant trust services criteria.

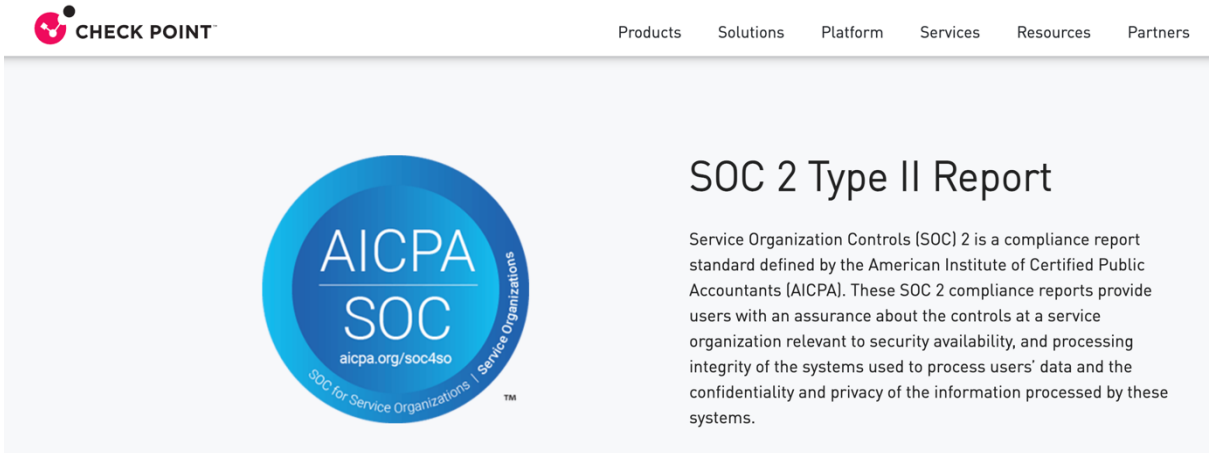
Check Point's SOC 2 Type II coverage supports controls relevant to security, availability, processing integrity, confidentiality, and privacy. These controls align with the State's requirement for a SaaS platform that provides platform-level data protection, access control, encryption in transit, encryption at rest, and third-party compliance validation.

The public Check Point SOC 2 Type II compliance page is provided as supporting documentation with this submission. The full SOC 2 Type II report is a controlled compliance document and will be made available through Check Point's standard trust,

compliance, NDA, or authorized request process during evaluation or upon request by the State.

Consultadd also maintains its own security-focused delivery controls for proposal support, coordination, and implementation assistance. Consultadd's organizational credentials include ISO 27001, SOC 2 Type II, CMMC alignment/readiness, HIPAA, and FERPA compliance practices, which support secure public-sector delivery and coordination.

The Check Point SOC 2 Type II public compliance page is included as a supporting reference in this submission, and the full controlled report will be made available through Check Point's authorized compliance-access process during evaluation or upon State request.



7. DEPLOYMENT TIMELINE

Consultadd understands that WVOT requires a rapid deployment approach that supports onboarding and full-mailbox API verification in under 24 hours without disrupting active State communications. The proposed solution is designed for fast cloud-based activation because it uses API-based integration with Google Workspace rather than MX record changes, mail-flow rerouting, local infrastructure deployment, or gateway cutover.

The proposed deployment approach will include:

1. confirmation of administrative access and required Google Workspace permissions;
2. validation of the State's mailbox scope and protection policies;
3. API authorization and configuration;
4. activation of core detection policies;
5. mailbox protection verification;
6. validation of reporting, alerts, and remediation workflows;
7. confirmation that the protected mailbox population is active under the proposed solution.

Consultadd will complete deployment activities in coordination with WVOT's technical stakeholders, including required Google Workspace administrative access, API authorization, and approval steps. The proposed solution supports onboarding and full-mailbox API verification in under 24 hours without disrupting active State communications. Deployment will be completed through authorized Google Workspace API integration and does not require MX record changes, gateway cutover, mail relay routing, or appliance deployment.

8. SUPPORT, UPDATES, AND INCIDENT RESPONSE AUTOMATION

The proposed annual SaaS subscription includes Check Point Advanced Protect capabilities, product updates, direct access to vendor-backed Tier 3 advanced support, and core incident response automation features for supported email threat detection and remediation workflows.

Consultadd will serve as the State's contracting and coordination point, providing communication, issue tracking, escalation coordination, and support management throughout the contract period. This approach gives WVOT a clear path for product-related assistance while ensuring the proposed solution remains aligned to the State's operational needs throughout Year 1 and optional renewal Years 2, 3, and 4.

9. SCOPE CLARIFICATIONS

Consultadd's proposed pricing is based on Check Point Advanced Protect for Google Workspace, SKU CPI-INF-BAS-C100, for advanced email security and core detection across the State's Google Workspace mailboxes.

Separate add-on modules for Data Loss Prevention and user-facing email encryption are not included in the proposed base pricing unless requested by the State as an optional enhancement or future change order. Platform-level security controls, including encryption in transit, encryption at rest, access control, and SaaS data-protection safeguards, are included as part of the proposed solution.

Pricing is based on the estimated mailbox quantity identified in the CRFQ. The estimated 22,000 mailboxes include licensed user mailboxes and potential shared, delegated, resource, and service-account mailboxes within the State's Google Workspace environment. Actual usage may be higher or lower, and the final billing quantity will follow the State's actual usage and contract terms as applicable.

ASSUMPTIONS AND CLARIFICATIONS

- Consultadd's proposed pricing is based on Check Point Advanced Protect for Google Workspace, SKU CPI-INF-BAS-C100, proposed as the Core Detection per Mailbox solution.
- Pricing is based on the CRFQ's estimated quantity of approximately 22,000 mailboxes, including licensed user mailboxes and potential shared, delegated, resource, and service-account mailboxes within the State's Google Workspace environment. Actual usage may be higher or lower, and the estimated quantity is not guaranteed by the State.
- Pricing is structured as an annual per-mailbox SaaS subscription for Year 1 and optional renewal Years 2, 3, and 4.
- The proposed base pricing includes the Check Point Advanced Protect license, product updates, direct access to vendor-backed Tier 3 advanced support, and core email threat detection, remediation, and incident response automation capabilities available under the proposed SKU.
- The proposed solution operates through native Google Workspace API integration and does not require MX record changes, gateway routing, mail relay routing, cloud proxy routing, or on-premises appliance deployment.
- The proposed solution supports onboarding and full-mailbox API verification in under 24 hours without disrupting active State communications.
- Separate Data Loss Prevention add-on modules are not included in the proposed base pricing unless requested by the State as an optional enhancement, add-on, or change order.
- Separate user-facing email encryption add-on modules are not included in the proposed base pricing unless requested by the State as an optional enhancement, add-on, or change order.
- Platform-level SaaS security controls, including encryption in transit, encryption at rest, access control, and applicable data-protection safeguards, are included as part of the proposed solution.
- Consultadd will coordinate product support, escalation assistance, implementation guidance, compliance materials, and ongoing communication with Check Point as part of the proposed delivery and support model.

EXCEPTIONS AND CLARIFICATIONS

Consultadd's proposal, pricing, implementation schedule, support model, and delivery commitments are based on the assumptions and clarifications below. These items address commercial terms only and do not modify any mandatory technical specification or any requirement that cannot be waived under West Virginia law. Consultadd requests that the final contract reflect the following commercially reasonable terms.

1. THIRD PARTY SAAS AND INTELLECTUAL PROPERTY

The State retains ownership of State data. Check Point and other third party products, software, services, documentation, application programming interfaces, configurations, and related intellectual property remain the property of their respective owners and are governed by the applicable license, subscription, support, and use terms. Consultadd retains ownership of its preexisting tools, templates, methods, workflows, documentation, and know how. No ownership interest in third party intellectual property or Consultadd background intellectual property is transferred. Manufacturer warranties, support commitments, and indemnities will be passed through to the State to the extent made available by the manufacturer.

2. LIMITATION OF LIABILITY

To the fullest extent permitted by West Virginia law, Consultadd's total aggregate liability arising from or relating to the contract will not exceed the fees paid or payable to Consultadd during the twelve months preceding the event giving rise to the claim. Liability arising from a breach of confidentiality, data privacy, data security obligations, or a security incident caused by Consultadd will not exceed two times that amount. These limits do not apply to fraud or willful misconduct. Consultadd will not be liable for indirect, incidental, special, punitive, consequential, lost profit, lost revenue, loss of goodwill, loss of business, or business interruption damages.

3. SECURITY INCIDENT RESPONSIBILITY

Consultadd is responsible for a security incident only to the extent caused by Consultadd controlled systems, Consultadd personnel, approved subcontractors, or Consultadd's failure to meet agreed security obligations. Consultadd is not responsible for incidents caused by State systems, State credentials, State users, State directed configurations, or third party systems outside Consultadd's control. Incident notification and response obligations will apply after Consultadd becomes aware of and confirms an incident involving State data within a Consultadd controlled system.

4. SUBSCRIPTION INVOICING AND THIRD PARTY COMMITMENTS

Consultadd's pricing assumes that annual SaaS subscription and license fees may be invoiced at activation and at the start of each renewal term, unless the applicable manufacturer quote states otherwise. Once ordered, third party subscriptions are noncancelable and nonrefundable except to the extent the manufacturer permits cancellation or refund.

Implementation and other professional services will be invoiced monthly in arrears or upon completion of an agreed milestone. The State will pay all undisputed amounts in accordance with applicable West Virginia payment requirements.

5. CURE RIGHTS AND TERMINATION PAYMENTS

Before termination for cause or the exercise of default remedies, Consultadd will receive written notice describing the material breach and thirty days to cure. The cure period for an undisputed payment default will be fifteen business days. Immediate termination will be limited to fraud, willful misconduct, a material violation of law, an imminent security risk, or circumstances in which immediate action is required by law. If the State terminates for convenience, nonappropriation, or suspension, Consultadd will be paid for services performed through the effective date, approved work in progress, transition services, and noncancelable third party or pass through costs incurred in reliance on the contract.

6. STATE DEPENDENCIES AND CHANGE CONTROL

Consultadd's schedule, pricing, staffing, and service commitments depend on the State's timely provision of required access, data, approvals, administrative permissions, technical personnel, testing support, and third party cooperation. A State caused delay or unmet dependency will extend affected dates by the period reasonably required to address the impact. Any material change to scope, mailbox volume, integrations, security obligations, service levels, or manufacturer costs will require a written change order or amendment signed by authorized representatives of both parties before the changed work is required.

7. INSURANCE

Consultadd will maintain commercially reasonable insurance for the services and will provide certificates of insurance and available endorsements upon request. Insurance obligations do not expand Consultadd's liability, waive an agreed limitation of liability, or create obligations beyond the applicable insurance policies and the agreed contractual risk allocation.

consultadd
Public Services

Thank You For Considering Our Proposal

Contact No.
+1 888 771 9958

Email Address
publicservices@consultadd.com

Website:
consultaddpublicservices.com

HQ Address
175 Greenwich Street, 38th Floor, New York, NY, 10007