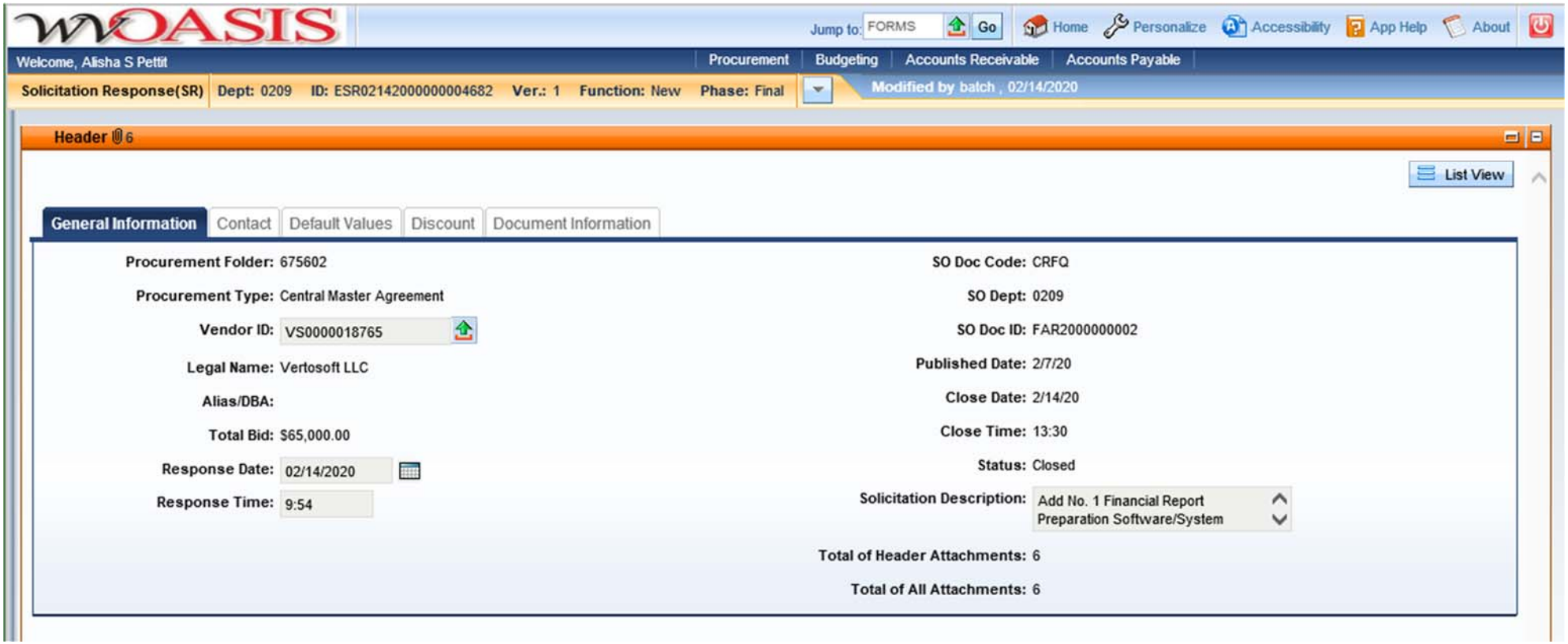
The following documentation is an electronically-submitted vendor response to an advertised solicitation from the *West Virginia Purchasing Bulletin* within the Vendor Self-Service portal at ***wvOASIS.gov***. As part of the State of West Virginia's procurement process, and to maintain the transparency 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.


wvOASIS
Jump to: FORMS Go
Home
Personalize
Accessibility
App Help
About
Welcome, Alisha S Pettit
Procurement
Budgeting
Accounts Receivable
Accounts Payable
Solicitation Response(SR) Dept: 0209 ID: ESR02142000000004682 Ver.: 1 Function: New Phase: Final
Modified by batch , 02/14/2020
Header 6
List View
General Information
Contact
Default Values
Discount
Document Information
Procurement Folder: 675602
Procurement Type: Central Master Agreement
Vendor ID: VS0000018765
Legal Name: Vertosoft LLC
Alias/DBA:
Total Bid: $65,000.00
Response Date: 02/14/2020
Response Time: 9:54
SO Doc Code: CRFQ
SO Dept: 0209
SO Doc ID: FAR2000000002
Published Date: 2/7/20
Close Date: 2/14/20
Close Time: 13:30
Status: Closed
Solicitation Description: Add No. 1 Financial Report Preparation Software/System
Total of Header Attachments: 6
Total of All Attachments: 6

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

State of West Virginia
Solicitation Response

Proc Folder : 675602

Solicitation Description : Add No. 1 Financial Report Preparation Software/System (CAFR

Proc Type : Central Master Agreement

Date issued	Solicitation Closes	Solicitation Response	Version
	2020-02-14 13:30:00	SR 0209 ESR02142000000004682	1

VENDOR

VS0000018765

Vertosoft LLC

Solicitation Number: CRFQ 0209 FAR2000000002

Total Bid : $65,000.00 **Response Date:** 2020-02-14 **Response Time:** 09:54:40

Comments:

FOR INFORMATION CONTACT THE BUYER

Melissa Pettrey

(304) 558-0094
melissa.k.pettrey@wv.gov

Signature on File **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	Implementation/Installation & First Year Maintenance/Support	1.00000	EA	$65,000.000000	$65,000.00

Comm Code	Manufacturer	Specification	Model #
43231500			

Extended Description : Implementation and Installation to Acceptance and First Year Maintenance Support Warranty/Hosting

STATE OF WEST VIRGINIA
Purchasing Division

PURCHASING AFFIDAVIT

CONSTRUCTION CONTRACTS: Under W. Va. Code § 5-22-1(i), the contracting public entity shall not award a construction contract to any bidder that is known to be in default on any monetary obligation owed to the state or a political subdivision of the state, including, but not limited to, obligations related to payroll taxes, property taxes, sales and use taxes, fire service fees, or other fines or fees.

ALL CONTRACTS: Under W. Va. Code §5A-3-10a, no contract or renewal of any contract may be awarded by the state or any of its political subdivisions to any vendor or prospective vendor when the vendor or prospective vendor or a related party to the vendor or prospective vendor is a debtor and: (1) the debt owed is an amount greater than one thousand dollars in the aggregate; or (2) the debtor is in employer default.

EXCEPTION: The prohibition listed above does not apply where a vendor has contested any tax administered pursuant to chapter eleven of the W. Va. Code, workers' compensation premium, permit fee or environmental fee or assessment and the matter has not become final or where the vendor has entered into a payment plan or agreement and the vendor is not in default of any of the provisions of such plan or agreement.

DEFINITIONS:

"Debt" means any assessment, premium, penalty, fine, tax or other amount of money owed to the state or any of its political subdivisions because of a judgment, fine, permit violation, license assessment, defaulted workers' compensation premium, penalty or other assessment presently delinquent or due and required to be paid to the state or any of its political subdivisions, including any interest or additional penalties accrued thereon.

"Employer default" means having an outstanding balance or liability to the old fund or to the uninsured employers' fund or being in policy default, as defined in W. Va. Code § 23-2c-2, failure to maintain mandatory workers' compensation coverage, or failure to fully meet its obligations as a workers' compensation self-insured employer. An employer is not in employer default if it has entered into a repayment agreement with the Insurance Commissioner and remains in compliance with the obligations under the repayment agreement.

"Related party" means a party, whether an individual, corporation, partnership, association, limited liability company or any other form or business association or other entity whatsoever, related to any vendor by blood, marriage, ownership or contract through which the party has a relationship of ownership or other interest with the vendor so that the party will actually or by effect receive or control a portion of the benefit, profit or other consideration from performance of a vendor contract with the party receiving an amount that meets or exceed five percent of the total contract amount.

AFFIRMATION: By signing this form, the vendor's authorized signer affirms and acknowledges under penalty of law for false swearing (*W. Va. Code* §61-5-3) that: (1) for construction contracts, the vendor is not in default on any monetary obligation owed to the state or a political subdivision of the state, and (2) for all other contracts, that neither vendor nor any related party owe a debt as defined above and that neither vendor nor any related party are in employer default as defined above, unless the debt or employer default is permitted under the exception above.

WITNESS THE FOLLOWING SIGNATURE:

Vendor's Name: Vertosoft LLC

Authorized Signature: _____ Date: 2-14-2020

State of Virginia

County of Loudoun, to-wit:

Taken, subscribed, and sworn to before me this 14 day of February, 2020.

My Commission expires 9.30, 2021.

AFFIX SEAL HERE

NOTARY PUBLIC _____

Annemarie Athey
NOTARY PUBLIC
Commonwealth of Virginia
Reg. #7546180
My Commission Expires 9/30/2021

Workiva

WORKIVA, INC.

Cloud-Based Collaboration Solutions and Support Operations

System and Organization Controls (SOC) for Service Organizations Report
for the period of November 1, 2018 to October 31, 2019

Grant Thornton

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

I. Report of Independent Service Auditors 1

II. Workiva, Inc.'s Assertion 4

III. Cloud-Based Collaboration Solutions and Support Operations' Description of its System and Controls 6

A. Overview of Workiva, Inc. 6

B. Scope of the Description 6

C. Internal Control Framework 6

D. Control Activities 10

E. Additional Information about Management's Description 15

F. Subservice Organizations 15

G. User Entity Controls 16

IV. Description of Workiva, Inc.'s Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results 19

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor 19

B. Control Objectives, Control Activities, and Tests Performed 20

GRANT THORNTON LLP
1201 Walnut Street, Suite 2200
Kansas City, MO 64106

D +1 816 412 2400
F +1 816 412 2404

I. Report of Independent Service Auditors

Board of Directors and Management
Workiva, Inc.

Scope

We have examined Workiva, Inc.'s (the "Company") description of its Cloud-Based Collaboration Solutions and Support Operations (the "System") titled "Workiva, Inc.'s Description of System and Controls" for processing user entities' transactions ("description") throughout the period November 1, 2018 to October 31, 2019 (the "specified period") and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "Workiva, Inc.'s Assertion." The controls and control objectives included in the description are those that management of the Company believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the System that are not likely to be relevant to user entities' internal control over financial reporting.

The Company uses two subservice organizations, Google LLC ("Google"), and Amazon Web Services ("AWS"), to provide data hosting services. The description in Section III of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organizations. The description also indicates that certain control objectives specified by the Company can be achieved only if complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. Our examination did not extend to controls of the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company'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

In Section II of this report, the Company has provided an assertion about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is 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; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives; selecting the criteria stated in the assertion; and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

Grant Thornton

Service auditor's responsibilities
Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements (ISAE) 3402, *Assurance Reports on Controls at a Service Organization*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the specified period. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria in management's assertion;
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description;
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved; and
- evaluating the overall presentation of the description, the suitability of the control objectives stated in the description, and the suitability of the criteria specified by the service organization in its assertion.

Inherent limitations
The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the System that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Grant Thornton

Opinion

In our opinion, in all material respects, based on the criteria described in Workiva, Inc.'s assertion:

a. The description fairly presents the Cloud-Based Collaboration Solutions and Support Operations system that was designed and implemented throughout the period November 1, 2018 to October 31, 2019.
b. The controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2018 to October 31, 2019 and subservice organizations and user entities applied the complementary controls assumed in the design of Workiva, Inc.'s controls throughout the period November 1, 2018 to October 31, 2019.
c. The controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period November 1, 2018 to October 31, 2019 if complementary subservice organization and user entity controls assumed in the design of Workiva, Inc.'s controls operated effectively throughout the period November 1, 2018 to October 31, 2019.

Restricted use

This report, including the description of tests of controls and results thereof in Section IV of this report, is intended solely for the information and use of management of the Company, user entities of the Company's System during some or all of the specified period, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be, and should not be, used by anyone other than these specified parties.

Grant Thornton LLP

Kansas City, MO
December 17, 2019

Workiva

II. Workiva, Inc.'s Assertion

We have prepared the description of Workiva, Inc.'s (the "Company") Cloud-Based Collaboration Solutions and Support Operations system (the "System") for processing user entities' transactions throughout the period November 1, 2018 to October 31, 2019 (the "specified period"), for user entities of the System during some or all of the specified period and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organizations and user entities of the System themselves, when assessing the risks of material misstatements of the user entities' financial statements.

The Company uses two subservice organizations, Google LLC ("Google"), and Amazon Web Services ("AWS"), to perform data hosting services. The description includes only the control objectives and related controls of the Company and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by the Company can be achieved only if the complementary subservice organization controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of the Company's controls are suitably designed and operating effectively, along with the related controls at the Company. The description does not extend to the controls of the user entities.

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

A. The description fairly presents the System made available to user entities of the System during some or all of the specified period for processing their transactions as it relates to controls that are likely to be relevant to user entities' internal control over financial reporting. The criteria we used in making this assertion were that the description:

    1. Presents how the system made available to user entities of the system was designed and implemented to process relevant user entity transactions, including, if applicable:

        a. The type of services provided, including, as appropriate, the classes of transactions processed;

        b. The procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system;

c. The information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities;

d. How the system captures and addresses significant events and conditions other than transactions;

e. The process used to prepare reports or other information for user entities;

f. Services performed by a subservice organization, if any, including whether the inclusive method or carve-out method has been used in relation to them;

g. The specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls; and

h. Other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

2. Includes relevant details of changes to the service organization's system during the specified period.

3. Does not omit or distort information relevant to the service organization's system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and their user auditors and may not, therefore, include every aspect of the System that each individual user entity of the System and its auditor may consider important in its own particular environment.

B. The controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the specified period to achieve those control objectives if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the specified period. The criteria we used in making this assertion were that:

1. The risks that threaten the achievement of the control objectives stated in the description have been identified by management of the Company;

2. The controls identified in the description would, if operating effectively, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

3. The controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

III. Cloud-Based Collaboration Solutions and Support Operations' Description of its System and Controls

A. Overview of Workiva, Inc.

Workiva (NYSE:WK) delivers Wdesk, an intuitive cloud platform that modernizes how people work within thousands of organizations, including over 75 percent of the 500 largest U.S. corporations by total revenue. Wdesk is built upon a data management engine, offering controlled collaboration, data connections, granular permissions, and a full audit trail. Wdesk helps mitigate risk, improves productivity, and gives users confidence in their data-driven decisions. For more information, visit workiva.com.

B. Scope of the Description

This description addresses only Workiva, Inc.'s Cloud-Based Collaboration Solutions and Support Operations system provided to user entities via the Wdesk system. The description is intended to provide information for user entities of the Cloud-Based Collaboration Solutions and Support Operations system and their independent auditors who audit and report on such user entities' financial statements or internal control over financial reporting, to be used in obtaining an understanding of the Cloud-Based Collaboration Solutions and Support Operations and the controls over that system that are likely to be relevant to user entities' internal control over financial reporting. The description of the system includes certain business process controls and IT general controls that support the delivery of Workiva's Cloud-Based Collaboration Solutions and Support Operations.

Wdesk is available as a subscription service. The company also offers customers support and professional services. Wdesk was created by experienced accountants, engineers, and entrepreneurs dedicated to helping public and private companies reduce time, risk, and costs associated with business reporting.

Occasionally, Workiva may make features or products available to select customers under a "Beta" or "Customer Development Program" agreement. These are not in scope for this report and would be addressed by a separate customer agreement, as appropriate.

C. Internal Control Framework

This section provides information about the five interrelated components of internal control at Workiva, including Workiva's:

- control environment,
- risk assessment process,
- monitoring activities,

- information and communications, and
- control activities.

1. Control Environment

The control environment sets the tone of an organization, influencing the control awareness of the organization. The control environment is embodied by the organization's awareness of the need for controls and the emphasis given to the appropriate controls through management's actions supported by its policies, procedures, and organizational structure.

a. Management Philosophy

The control environment at Workiva is process-based, situated within an organizational structure designed to optimize the delivery of services to all customers. Executive and senior leadership provide governance and play an integral role in establishing the core values and culture of the organization. The Chief Compliance Officer provides leadership and oversight of controls and security to execute the governing principals set forth by the Executive Management team. This role also provides for the auditing of processes and controls, actively reviewing key areas on a continual basis.

Functional departments engage each employee in the controls process, providing an environment that facilitates a flow of knowledge, empowers execution, and ensures a clear understanding of responsibilities and obligations. Core production departments include Research and Development, Infrastructure and Reliability, Customer Success, and Professional Services. Supporting departments include Corporate Marketing, Human Asset Management, Accounting, Finance, Corporate Administration, Information Technology, Quality Assurance, and Sales.

b. Security Management

Workiva maintains an Information Security program designed to protect the security, confidentiality, integrity, availability, and privacy of its computing infrastructure and associated customer confidential data. It is the policy of Workiva to establish management direction and define procedural requirements for Information Security to ensure the appropriate protection of information and assets of the organization and its customers in a manner commensurate with its confidentiality, value, and criticality while also meeting regulatory requirements. Workiva therefore utilizes a policy-driven information security architecture approach that is coordinated and managed by the Information Technology department and integrated into the Information Security risk management process. Implementation and execution is further facilitated through cross-functional groups that are brought together to address key requirements. Workiva Information Security policies are reviewed and approved by management, and received and signed by all employees.

Information security at Workiva is a team effort, involving the participation and support of every employee. This program includes:

- Provisions for the education of employees on information security awareness
- Establishment, assessment, and maintenance of policies and procedures
- Investigation of suspected abuses of Workiva information systems, information, and communication mediums
- A functional and clearly communicated Incident Management Standard.

c. Hiring Practices and Staff Development

Workiva employee and consultant hiring procedures include background checks. Termination procedures ensure return and/or destruction of any and all company and customer information and suspension of access to company networks and software systems. In addition, termination of technical and customer support personnel may require additional action including account suspension for enterprise software systems for which they may have administrative access.

Workiva Human Asset Management team relies upon a clearly defined hiring process that includes the following steps:

- Initiate recruiting efforts as necessary
- Complete pre-screening of resumes
- Select interview candidates
- Set up and conduct interviews
- Make final candidate selection
- Request authorization to complete background checks and check references
- Check references
- Complete background checks
- Make written employment offer
- Upon receiving signed offer letter, prepare all remaining employment documents, including Confidentiality and Inventions Assignment Agreement and I9 Form

On employee's first day of work, employee is provided an orientation session that includes an Information Security session given by a member of the Information Security team and is given access to WLife (a compilation of corporate policies) and Customer Confidentiality and Securities Trading Policy. Employees are asked to sign and acknowledge receipt and compliance with these documents.

Recurring training occurs throughout the year, specifically making sure that personnel are trained on security awareness and trading compliance annually. Employees review the code of conduct and acknowledge receipt to be in compliance with WLife on an annual basis. Users with elevated levels of access undergo additional training that address specific Security and Confidentiality requirements in relation to their job functions on an annual basis.

2. Risk Assessment Process

Workiva management understands the benefits of proactive risk management and maintains a formal risk management program. This program relies on input from business units, support resources, and executive management to identify, assess, and mitigate risk across the business. Core functional departments, such as Research & Development and Customer Success, identify and report situations where risk levels are outside of established organizational tolerance levels. The Information Security team takes a proactive approach and conducts audits and assessments to ensure controls are adequate and operating as designed.

The Workiva control environment is subject to internal and external assessments. The Workiva Information Security team maintains a framework to facilitate risk review and validation using internal testing as well as vulnerability assessments by third parties. The team reviews all

security-related issues during product development and prior to deployment, and works to develop, review, and disseminate Information Security-related policies, standards, and procedures.

Workiva has an established Incident Management Standard that outlines communication and escalation in the event of any type of event outside of normal business operations.

3. Monitoring Activities

Workiva recognizes the need to be alert to external risks and vigilant in looking for potential issues or active incidents. Workiva evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its ongoing risk assessment and management process and revises these when necessary to meet changing commitments and requirements. System architecture diagrams depicting details of production systems and the system boundary are maintained for use in describing and auditing the Wdesk environment.

Workiva performs the following incident and risk management activities on an annual basis:

- Conducts a risk assessment and business impact analysis to evaluate risks to the Wdesk environment and to ensure the appropriateness of controls.
- Performs a business continuity exercise that includes both technical and pandemic scenarios.
- Trains members of the Incident Response Team to ensure awareness of proper escalation paths and criteria.

The Incident Management Standard addresses identification, documentation, resolution, communication, and escalation of both operational and security incidents. Active monitoring provides key information used to identify potential incidents. Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and the use of an anonymous third-party administered ethics hotline. Workiva policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct. Monitoring software is used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes and alert operations personnel for remediation.

Proactive third-party vulnerability assessments are performed semi-annually and internal assessments are performed monthly on Workiva applications to identify additional potential exposures. Additionally, internal reviews of compliance with information security policies are performed on a monthly basis. Internal testing and in-house tools are also used as a component of the quality assurance process to maximize identification of potential risks.

This proactive stance applies to all aspects of the Workiva infrastructure. Anti-malware programs are installed on all company-issued laptops. All devices for users with access to Restricted data are encrypted and prevented from writing to removable media and these users are required to use their Workiva device when handling Restricted data. Workiva works closely with its vendors to ensure they have equally stringent Incident and Risk Management programs in place. Vendors providing mission-critical services in support of the production environment are reviewed annually by Workiva to identify both capability and risk. A mission critical service is defined as one that requires continuous availability. Breaks in service are intolerable and immediately and significantly damaging. Agreements with sub-processors of restricted-level customer information include language to address security and confidentiality requirements.

4. Information and Communications

Workiva applies various communication strategies, both internal and customer facing, to ensure that information is effectively distributed, available, and used in implementing and executing actions to achieve organizational goals, as well as delivering expected value to customers.

Internal

Workiva utilizes several mechanisms to communicate information across the organization. Several of the key tenets of communication within the organization encourage content to be timely, relevant, clear, complete, and appropriate. An intranet is used to communicate general information to employees, including policies, procedures, and general business updates. Additional tools include email, new hire orientation, training, regular management meetings, and video broadcasts. Any product service interruptions or changes are promptly communicated internally between departments according to the Incident Management Standard, and depending upon impact to the customer experience, communicated directly to impacted parties.

External

The Customer Success department provides the primary direct communication interface for Workiva customers. Telephone, email, and cell phone provide direct access for customers to contact Workiva with any inquiry. Proactive communications are also initiated to alert customers of incidents or significant changes to the application or operating environment. Customers are also provided a mechanism via Wdesk to request enhancements and provide feedback.

D. Control Activities

The service organization has developed a variety of policies and procedures including related control activities to help ensure the service organization's objectives are carried out and risks are mitigated. Control activities are performed at a variety of levels throughout the organization and at various stages during the relevant business process. Controls may be preventive or detective in nature and may encompass a range of manual and automated controls. Duties and responsibilities are allocated among personnel to help ensure that a proper segregation of duties is maintained.

A formal program is in place to review and update the service organization's policies and procedures on at least an annual basis. Any changes to the policies and procedures are reviewed and approved by management and communicated to employees.

1. Organization and Management

Workiva information security starts with people and processes. Security is built into corporate culture from the very beginning. Job roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors. Job descriptions are reviewed by Workiva management on an annual basis. Key personnel in Workiva management comprise an Information Security Risk committee. This team is responsible for information security throughout the business and is divided into functional areas, including application security, IT security, operational security, and governance. This team meets monthly to review information security, risk, and compliance issues.

Workiva develops, disseminates, and periodically reviews and updates a formal, documented Information Security Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

Workiva implements a number of internal policies and procedures to ensure that customer information is kept confidential and secure. Corporate governance policies and agreements include the following:

- Information Security Program Charter
- Application Development Security Policy
- Business Continuity Policy
- Change Management Policy
- Customer Data Access Policy
- Encryption Policy
- Endpoint Device Security Policy
- Identity & Access Management Security Policy
- Incident Management Policy
- Information Classification Standard
- Information Assessment Management Policy
- Personnel Security Policy
- Physical Security Policy
- Risk Management Policy
- Security Assessment Policy
- Server & Network Device Security Policy
- Third-Party Relationships Security Policy
- Internal IT and Wdesk Procedures
- Third-Party Non-Disclosure Agreement
- Third-Party Security Standard Consultant Agreement
- Customer Confidentiality and Securities Trading Policy
- WLife Employee Handbook (including portions of the above).

Workiva maintains these policy and procedure documents for at least six years. Policies are included in WLife, and available on the company intranet. Procedures are published on the company intranet.

2. Trading Compliance

Workiva has a comprehensive program to ensure that private customer information is not disclosed to outside parties or misused by employees.

Employees are required to disclose their personal holdings upon commencement of employment. Employees or consultants who violate the Customer Confidentiality and Securities Trading Policy are subject to immediate disciplinary action up to and including dismissal. During the course of business, Workiva employees and consultants may become aware of material non-public

information for a publicly traded company. Federal securities laws prohibit any person from buying and selling securities while in possession of such information. Workiva has implemented a strict Customer Confidentiality and Securities Trading Policy along with internal processes and education programs that support enforcement and awareness.

Publicly traded companies, whether a direct customer or not, are placed on a No-Trade List the moment relevant business activity warrants this designation. No-Trade designated companies are tracked in the enterprise sales and support database. This list of No-Trade designated companies is updated daily and made available to all employees and consultants of Workiva via the company intranet. Each employee and contractor is required to sign a confidentiality statement, agreeing not to disclose proprietary or confidential information, including customer confidential information.

3. Logical Access Security

Workiva defines acceptable channels through which restricted-level customer data can be transferred that adhere to the security and confidentiality obligations and trains employees on these channels. Access to systems that contain restricted level customer data requires users to authenticate via a single sign-on system. System administration tasks require the use of a multi-factor authenticated VPN to access consoles.

Production systems conform to documented configuration hardening guidelines, including firewall rules. These systems are audited for conformance with the hardening guidelines on a weekly basis with the use of automated scans. Firewalls rules are reviewed for appropriateness and approved by management on a semi-annual basis.

The granting or modification of access rights is based on the concept of least privilege and must be authorized and approved by the user's functional manager and the application owner. Approvals are requested, tracked, and resolved by workflow management tools. Administrative production system access is granted only to individuals who have been trained and require this level of access to perform required tasks. Access to production systems is removed by the system owner upon submission of a termination request by Human Asset Management. Users are required to utilize unique user IDs to access systems. Passwords adhere to the documented password policy, including complexity, length, re-use restrictions, and expiration requirements. Access to systems containing Restricted information makes use of two-factor authentication for Workiva personnel. User access is reviewed and certified by management on a semi-annual basis.

Customer user account management requests must be appropriately authorized per customer agreement.

4. Incident and Risk Management

Workiva recognizes the need to be alert to external risks and vigilant in looking for potential issues or active incidents. The Incident Management Standard addresses identification, documentation, resolution, communication, and escalation of both operational and security incidents. Active monitoring provides key information used to identify potential incidents. Proactive third-party vulnerability assessments are performed semi-annually and internal assessments are performed monthly on Workiva applications to identify additional potential exposures. Additionally, internal reviews of compliance with information security policies are performed on a monthly basis. Internal testing and in-house tools are also used as a component of the quality assurance process to maximize identification of potential risks.

This proactive stance applies to all aspects of the Workiva infrastructure. Anti-malware programs are installed on all company-issued laptops. All devices for users with access to restricted data are encrypted and prevented from writing to removable media and these users are required to use their Workiva device when handling restricted data. Workiva works closely with its vendors to ensure they have equally stringent Incident and Risk Management programs in place. Vendors providing mission-critical services in support of the production environment are reviewed annually by Workiva to identify both capability and risk. A mission critical service is defined as one that requires

continuous availability. Breaks in service are intolerable and immediately and significantly damaging.

5. Product Development and Change Management

Workiva uses a defined Software Development Life Cycle (SDLC) with an emphasis on functionality, quality, responsiveness, and security. This systematic approach includes a process to ensure that any changes to systems or applications are thoroughly reviewed, tested, approved, and well communicated.

The SDLC employs Agile software development practices designed to be nimble and responsive with customers and the market. Research & Development teams prioritize their work and maintain a queue of work that is planned and in-progress. Teams meet regularly to review their work with the larger organization, hold planning meetings, and hold retrospectives to review how they are working as a team and identify performance improvements going forward. Many teams also hold stakeholder meetings where they invite stakeholders to provide input on their future direction.

Updates to Wdesk are released on a regular basis as work is completed. Release Management verifies completion of all SDLC requirements for any code before it is used in the production environment.

Members of Research & Development, Information Technology, Infrastructure & Reliability, Quality Assurance, and Information Security with knowledge and training in software and Information Security are authorized as Security Reviewers. These individuals are involved in all phases of product development, and review changes to software code that is security-sensitive. This includes code involved in session management, access control, APIs that perform cross-platform calls, authentication, input validation, output encoding, secure transmission, audit logging, file uploads, XSS/CSRF protection, or encryption/hashing. Additions and modifications to this code are consistently reviewed and approved by authorized reviewers prior to being merged into the master codebase. An automated monitoring system, built and maintained by the Information Security team, is in place to help ensure items are appropriately flagged for security review. In addition, great care is taken during the design and prototyping phases of any feature set to identify architecture and implementation that may require security consideration. New feature sets requiring security consideration are subject to a full Information Security team assessment prior to production release.

Workiva leverages a combination of software development tools and a defined process to facilitate the flow, structure, communication, collaboration, and management of product development. Examples of this integration of tools and process include:

- Segregated development, testing, and production environments that are maintained for the security and integrity of the system.
- Project management tools and ticketing system that provide tracking of all projects from initiation to implementation. Work is tracked in order to provide a clear path for all team members, and a mechanism to adjust project parameters and requirements.
- Advanced automated and/or manual quality assurance testing tools that are used to maximize the operating capabilities of Wdesk.
- Development items that have security impact are identified and tracked in the project management/ticketing system. This allows issues/changes that have a potential security impact to be easily identified, and routed for code review, security review, and receive final sign-off by the Information Security team prior to release into production.
- The project management/ticketing system provides the functionality necessary to achieve and record all required management sign-offs prior to any code releases.

- Version control software used to manage current versions of source code for the in-scope applications. The ability to modify source code for the in-scope applications is restricted to appropriate personnel based on job function.

6. Physical Security Controls

Workiva offices are secured with a proximity badge system and are monitored with a system of high-resolution IP cameras. This security system controls access to non-public entrances, private areas, and restricted areas at all times and public entrances outside of business hours. Footage is captured 24/7, and is retained for 90 days. All facilities are equipped with shred bins and employees are trained to shred all paper containing even potentially confidential information.

Public entrances are staffed and monitored by a receptionist who manages a visitor sign-in log, ensures visitors complete a non-disclosure agreement, and issues visitor badges. Employees badge in and out at all entrances, and the times are recorded. Access to offices is maintained in conjunction with the Human Asset Management change process, and management performs a comprehensive access review annually.

Workiva performs a risk assessment of vendors' security and capabilities. This review is conducted commensurate with the level of information they have access to.

7. System Monitoring

Internally, Workiva utilizes both automated and periodic manual review systems to provide a high level of service and availability. Customers are provided with proactive monitoring tools within the Wdesk environment to review key activities, such as authentication, authorization, permissions, and document changes. Workiva and its partners use a combination of commercially available tools and custom tools to detect suspicious activity.

Examples of monitoring activities in each of these categories include:

Internal

- Logging and monitoring of SEC filing activities
- Application operating parameters and performance
- Application operation transaction exceptions
- System administration authentication and activity
- Application development activities and production changes
- Security incidents and security related development activities
- Application access reviews
- Regular internal audits and vulnerability assessments
- Periodic third-party security vulnerability assessments
- System log analysis review

Customer

- Authentication activities
- Application access reviews
- User additions
- Permissions and authorization changes

- Document change history
- User role changes

E. Additional Information about Management's Description

The Company has specified the control objectives and identified the controls that are designed to achieve the related control objectives. The specified control objectives and related controls are presented within Section IV of this report, "Description of Workiva, Inc.'s Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results," and are an integral component of the Company's description of its system as described within this section.

F. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve specific control objectives, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
Amazon Web Services ("AWS")	The Company uses Amazon Web Services for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications; and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following controls to help monitor the subservice organization: • An annual risk assessment review is conducted of vendors providing mission critical services in support of the production environment; and	CO 6*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Control Objective
	• Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	
Google, LLC ("Google")	The Company uses Google for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications; and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following controls to help monitor the subservice organization: • An annual risk assessment review is conducted of vendors providing mission critical services in support of the production environment; and • Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	CO 6*

* The achievement of design and operating effectiveness for this particular control objective assumes that complementary controls at this subservice organization are in place and are operating effectively to support and achieve this control objective.

G. User Entity Controls

Workiva, Inc.'s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company's system. It is not feasible for the control objectives to be solely achieved by the Company. Therefore, each user entity's internal control over financial reporting must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified within the table below, where applicable. Complementary user entity controls and their associated control objectives are included within the table below.

Management has highlighted control objectives in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls over financial reporting that are relevant to the Company's controls detailed in this report; however, such control considerations are not required to achieve design or operating effectiveness for the control objective. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities that provide a basis for the assertions underlying the financial statements and control environments for the Company's user entities.

User Entity Control	Associated Control Objective(s)
Customers are responsible for completeness, accuracy, and timeliness of the information that is created, manipulated, and filed in the process of using Wdesk.	CO 7*
Customers are responsible for administering and monitoring all user accounts with access to their data.	CO 3*
Customers are responsible for the logical security of all devices involved in the use of Wdesk that are used by customers or agents of the customer.	CO 3*
Customers are responsible for establishing and enforcing their own password security policy and enabling appropriate controls in Wdesk.	CO 3*
Customers are responsible for setting and maintaining document permissions on a per-section basis for editing and reading.	CO 3*
Customers are responsible for security and reliability of the connection to Wdesk.	CO 7*
Customers are responsible for Information Security training for all users with access to their data.	CO 7*
Customers are responsible for contacting and working cooperatively with Workiva if there are any issues with security including, but not limited to, unauthorized use of their password or account.	CO 4*
Customers are responsible for backing up data in accordance with their own relevant requirements.	CO 4
Customers are responsible for the physical security of all devices involved in the use of Wdesk that are used by customers or agents of the customer.	CO 6*
Customers are responsible for specifying one or more administrators who will have the appropriate rights and permissions to access the administrative tools provided with Wdesk.	CO 3*, CO 7*

User Entity Control	Associated Control Objective(s)
Customers are responsible for maintaining and communicating to Workiva the accurate Account Administrator contact information for all designated account administrators.	CO 7
Customers are expected to self-administer the desired level of document retention by backing up their critical data using the tools provided within Wdesk.	CO 4*

* This is a complementary user entity control and is required to achieve design and operating effectiveness for this particular control objective.

IV. Description of Workiva, Inc.'s Control Objectives and Related Controls and the Independent Service Auditor's Description of Tests of Controls and Results

A. Types and Descriptions of the Tests of Operating Effectiveness Provided by the Independent Service Auditor

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to assist auditors in planning the audit of user entities' financial statements or user entities' internal control over financial reporting and in assessing control risk for assertions in user entities' financial statements that may be affected by controls at the Company.

Our examination was limited to the control objectives and related controls specified by the Company in Sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations.

It is the responsibility of each user entity and its independent auditor to evaluate this information in conjunction with the evaluation of internal control over financial reporting at the user entity in order to assess the internal control environment. If the internal controls are not effective at a user entity, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the control objectives specified by the Company, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used within this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control

In addition, when using information produced (or provided by) the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

B. Control Objectives, Control Activities, and Tests Performed

Control Objective 1

Controls provide reasonable assurance that discipline, structure, and security awareness are an integral part of the organization and influence the control environment.

Control Activity		Tests Performed By Service Auditor	Results of Testing
1.1	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
1.2	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
1.3	Employees are trained on security awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry:** Inquired of the VP of HR to determine that employees were trained on Security Awareness and Customer Confidentiality and the Securities Trading Policy upon hire and annually.	No exceptions noted
		Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted

Control Objective 1

Controls provide reasonable assurance that discipline, structure, and security awareness are an integral part of the organization and influence the control environment.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
1.4	The organization performs a background check on individuals as a component of the hiring process and will decline to hire any individual with a felony conviction, or a conviction for theft or fraud. Workiva will review convictions for misdemeanors to determine whether they would compromise safety or security.	**Inquiry:** Inquired of the VP of HR to determine that the entity performed background checks on individuals as a component of the hiring process, as permissible in each country, and declined to hire any individual with a felony conviction, or a conviction for theft or fraud. In addition, the company reviewed convictions for misdemeanors to determine whether they would compromise safety or security.	No exceptions noted.
		Inspection: Inspected the background check report for a sample of new hires to determine that the entity performed background checks on individuals as a component of the hiring process, as permissible in each country, and will decline to hire any individual with a felony conviction, or a conviction for theft or fraud.	No exceptions noted.

Control Objective 2

Controls provide reasonable assurance that processes are in place to help ensure customer information is not disclosed to outside parties or misused by employees

	Control Activity	Tests Performed By Service Auditor	Results of Testing
2.1	The Compliance Officer maintains, approves and publishes a Customer Confidentiality & Securities Trading Policy.	**Inquiry:** Inquired of the EVP Chief Legal Officer to determine that the Compliance Officer maintained, approved and published a Customer Confidentiality & Securities Trading Policy.	No exceptions noted.
		Inspection: Inspected the Customer Confidentiality & Securities Policy to determine that the Compliance Officer maintained, approved and published a policy around confidentiality and securities trading.	No exceptions noted.
2.2	The organization maintains and publishes a Restricted Trade List.	**Inquiry:** Inquired of Troy Calkins, EVP Chief Legal Officer to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
		Inspection: Inspected the Restricted Trade List/No Trade List email to determine that the organization maintained and published a Restricted Trade List on the intranet.	No exceptions noted.
		Inspection: Inspected the script used to automatically update the Restricted Trade List to determine that the organization had a process to scan for and identify new accounts to add to the Restricted Trade List based on newly onboarded clients.	No exceptions noted.
		Inspection: Inspected the Insider Trading Policy to determine that a policy was in place to prohibit employees from engaging in insider trading and defined a process to allow employees to request permission to conduct trading activities.	No exceptions noted.
2.3	Employees and contractors are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	**Inquiry:** Inquired of the VP of HR to determine that employees and contractors were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.
		Inspection: Inspected the evidence of confidentiality agreements for the selected samples to determine that employees and contractors were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.
2.4	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry:** Inquired of the VP of HR to determine that employees were trained on Security Awareness and Customer Confidentiality and the Securities Trading Policy upon hire and annually.	No exceptions noted

Control Objective 2 Controls provide reasonable assurance that processes are in place to help ensure customer information is not disclosed to outside parties or misused by employees			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
		Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
2.5	Customer Success leadership (Workiva platform Super Administrators) complete annual training specific to the risks and obligations of their role in administering accounts and users.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that Customer Success leadership (Workiva platform Super Administrators) completed annual training specific to the risks and obligations of their role in administering accounts and users.	No exceptions noted.
		Inspection: Inspected the certificate of completion for the Being a Wdesk Super Admin training for a sample of super administrators to determine that Customer Success leadership completed annual training specific to the risks and obligations of their role in administering accounts and users.	No exceptions noted.
		Inspection: Inspected the super admin training material to determine that the training content included information relevant to risks and obligations of the Customer Success leadership's role in administering accounts and users.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that system information is restricted to authorized and appropiate users.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
3.1	Users are required to utilize unique User IDs to access system resources.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that users were required to utilize unique User IDs to access system resources.	No exceptions noted.
		Observation: Observed the Senior Director of Information Security attempt to create a non-unique user ID within the single sign on tool, Okta, and not be permitted to complete the set-up to determine that users were required to utilize unique user IDs to access system resources.	No exceptions noted.
		Inspection: Inspected the user access listings for network and production systems to determine that users were required to utilize User IDs to access system resources, and that there were no duplicate userIDs.	No exceptions noted.
3.2	Password requirements for in-scope systems adhere to the documented Password Policy.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that password requirements for in-scope systems adhered to the documented Password Policy.	No exceptions noted.
		Inspection: Inspected the Password Policy within the Identity and Access Management Policy to determine that password requirements were defined for in-scope systems.	No exceptions noted.
		Inspection: Inspected the password settings for each in-scope system to determine that password requirements for in-scope systems adhered to the documented Password Policy.	No exceptions noted.
3.3	Logical access to Restricted Information requires the use of two-factor authentication.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that logical access to restricted information required the use of two-factor authentication.	No exceptions noted.
		Observation: Observed the Senior Director of Information Security login to the Workiva production systems and determined that two-factor authentication was used and was required to access system information, including restricted information.	No exceptions noted.

Control Objective 3

Controls provide reasonable assurance that system information is restricted to authorized and appropiate users.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the two-factor authentication configuration to determine that logical access to system information, including restricted information, required the use of two-factor authentication.	No exceptions noted.
3.4	Default user access is granted based on job responsibilities by department and approved by business unit management.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of HR to determine that default user access was granted based on job responsibilities by department and approved by business unit management.	No exceptions noted.
		Inspection: Inspected the HR profile for a sample of new hires to determine appropriate business unit management gave approval prior to hire and default access being granted.	No exceptions noted.
3.5	User access is reviewed and certified by management on a semi-annual basis.	**Inquiry:** Inquired of the Senior IT Risk & Compliance Analyst to determine that user access was reviewed and certified by management on a semi-annual basis.	No exceptions noted
		Inspection: Inspected the most recent user access review for the in-scope systems to determine that user access reviews were performed and certified by management semi-annually.	No exceptions noted
3.6	User access to Workiva's cloud networks and in-scope applications and databases is revoked within 2 business days of an employee's termination date.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
		Inspection: Inspected the ticket for a sample terminated employees and contractors and the access list to in-scope systems to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that IT operations and security related incidents are identified and managed to mitigate associated security risk.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
4.1	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry:** Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
4.2	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry:** Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
		Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
4.3	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
		Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
		Inspection: Inspected the the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
4.4	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that IT operations and security related incidents are identified and managed to mitigate associated security risk.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
4.5	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
		Inspection: Inspected the results vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
		Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
4.6	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry:** Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
		Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
4.7	Customer SEC filing activities are logged and monitored with automated alerts.	**Inquiry:** Inquired of the Senior Software Architect to determine that customer SEC filing activities were logged and monitored with automated alerts.	No exceptions noted.
		Inspection: Inspected the evidence of filing alerts to determine that customer SEC filing activities were logged and monitored with automated alerts.	No exceptions noted.
4.8	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to	**Inquiry:** Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

Control Objective 4

Controls provide reasonable assurance that IT operations and security related incidents are identified and managed to mitigate associated security risk.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
	log and automatically create a ticket for review.	**Inspection:** Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
		Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that changes in business software are managed through the appropriate level of planning, access, approval, and testing.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
5.1	System Development Life Cycle policies and procedures are in place.	**Inquiry:** Inquired of the Senior Software Architect to determine that System Development Life Cycle policies and procedures were in place.	No exceptions noted.
		Inspection: Inspected the Application Security Standard to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
		Inspection: Inspected the Development Security Review procedure and the SDLC process flow chart to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
5.2	Version control software is in place to manage current versions of source code for the in-scope applications. The ability to modify source code for the in-scope applications is restricted to appropriate personnel based on job function.	**Inquiry:** Inquired of the Senior Software Architect to determine that version control software was in place to manage current versions of source code for the in-scope applications and the ability to modify source code for the in-scope applications was restricted to appropriate personnel based on job function.	No exceptions noted.
		Observation: Observed the Senior Software Architect attempt to merge a change into production without appropriate Release Management approval and the change being blocked from release to production to determine that the ability to modify source code for the in-scope application was restricted appropriately.	No exceptions noted.
		Inspection: Inspected the list of users with access to modify source code and their job responsibilities to determine that the ability was restricted appropriately.	No exceptions noted.
5.3	Segregation of responsibilities for code changes to the production environment is maintained between development, code review, and release processes.	**Inquiry:** Inquired of the Senior Software Architect to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
		Inspection: Inspected the System Development Life Cycle process flow chart to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that changes in business software are managed through the appropriate level of planning, access, approval, and testing.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
		Inspection: Inspected the ticket for a sample of releases showing the individuals who performed code review and QA review and the automated release tool that pushed the release to production to determine that separate individuals performed code review, QA review, and release signoff showing segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
5.4	Quality assurance testing procedures are performed and documented for code changes to the production environment.	**Inquiry:** Inquired of the Senior Software Architect to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
		Inspection: Inspected the ticket for a sample of releases to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
5.5	Release Management verifies Development and Quality Assurance requirements have been met prior to release into production.	**Inquiry:** Inquired of the Senior Software Architect to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
		Observation: Observed the automated process to release changes to production to determine that release management verified development and quality assurance requirements were met prior to releasing the change into production and halted the release when certain requirements were not met.	No exceptions noted.
		Inspection: Inspected the ticket for a sample of releases to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
5.6	Separate Test, Development, and Production environments are maintained for the Workiva platform.	**Inquiry:** Inquired of the Senior Software Architect to determine separate test, development, and production environments were maintained for the Workiva platform.	No exceptions noted.
		Observation: Observed the test, development and production environments for the Workiva platform to determine that separate environments were maintained.	No exceptions noted.

Control Objective 5

Controls provide reasonable assurance that changes in business software are managed through the appropriate level of planning, access, approval, and testing.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
5.7	System changes that can impact the security of the system have security reviews performed and signed off by management prior to release into production.	**Inquiry:** Inquired of the Senior Software Architect to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
		Inspection: Inspected the Development Security Guidelines to determine that they documented the process around the security reviews performed for system changes impacting the security of the system.	No exceptions noted.
		Inspection: Inspected the evidence of security review and sign off samples to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.

Control Objective 6

Controls provide reasonable assurance that physical access to the corporate facilities and the off-site data center is properly controlled and managed.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
6.1	Access to operational work areas and computer rooms are controlled and appropriately secured.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that access to operational work areas and computer rooms was controlled and appropriately secured.	No exceptions noted.
		Inspection: Inspected the access list from the badge system to determine that access to operational work areas and computer rooms was controlled and appropriately secured.	No exceptions noted.
6.2	Exterior and telecommunication room entrances are monitored by cameras and recordings are retained for a 90 day period. (Tier I and II Sites)	**Inquiry:** Inquired of the Director of Information Technology to determine that exterior and telecommunication room entrances were monitored by cameras and recordings were retained for a 90 day period.	No exceptions noted.
		Observation: Observed the presence of cameras at the Workiva headquarters to determine that exterior and telecommunication room entrances were monitored by cameras.	No exceptions noted.
		Inspection: Inspected the camera monitoring console and the retention setting on the logs to determine that security cameras were in place to monitoring exterio and telecommunication room entrances at various Workiva locations, and that recordings were retained for a 90 day period.	No exceptions noted.
6.3	Visitors are required to sign in at the reception desk. (Tier I and II Sites)	**Inquiry:** Inquired of the Chief Administrative Officer to determine that visitors were required to sign-in at the reception desk.	No exceptions noted.
		Observation: Observed the visitor sign-in process at the Workiva headquarters during various visits to determine that visitors were required to sign in at the reception desk.	No exceptions noted.
		Inspection: Inspected the visitors log for multiple Workiva office locations to determine that visitors access was logged and retained.	No exceptions noted.
6.4	Visitors accessing areas where Restricted information is handled must sign a non-disclosure agreement. (Tier I and II Sites)	**Inquiry:** Inquired of the Chief Administration Officer to determine that visitors accessing areas where Restricted information was handled must sign a non-disclosure agreement.	No exceptions noted.

Control Objective 6 Controls provide reasonable assurance that physical access to the corporate facilities and the off-site data center is properly controlled and managed.			
Control Activity		**Tests Performed By Service Auditor**	**Results of Testing**
		Observation: Observed the visitor sign in process to determine that visitors accessing areas where restricted information was handled had to sign a non-disclosure agreement, which was a step in the visitor sign in process.	No exceptions noted.
		Inspection: Inspected the email receipt of the non-disclosure agreement signed by visitors to determine that it is automatically sent to the visitor by the logging tool upon signing in.	No exceptions noted.
6.5	Access to corporate facilities is reviewed on a semi-annual basis.	**Inquiry:** Inquired of the Director of Information Technology and the Compliance Auditor to determine that access to corporate facilities was reviewed on a semi-annual basis.	No exceptions noted.
		Inspection: Inspected the most recent review of physical access to Workiva facilities to determine that access to corporate facilities was reviewed on a semi-annual basis and actions taken to address issues noted.	No exceptions noted.
6.6	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
		Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that data is appropriately secured and protected from unauthorized or unintentional use, modification, addition, or deletion.

	Control Activity	Tests Performed By Service Auditor	Results of Testing
7.1	Customer user account management requests must be appropriately authorized per customer agreement.	**Inquiry:** Inquired of the Director of Global Services Operations to determine that customer user account management requests must be appropriately authorized per customer agreement.	No exceptions noted.
		Inspection: Inspected the Customer Data Access Policy to determine that customer user account management requests were required to be appropriately authorized per customer agreement.	No exceptions noted.
		Inspection: Inspected the client request for a sample of new customer access granted to determine that customer user account management requests were appropriately authorized per customer agreement.	No exceptions noted.
7.2	Customer data is restricted to only authorized users.	**Inquiry:** Inquired of the Director, Global Services Operations to determine that customer data was restricted to only authorized users.	No exceptions noted.
		Observation: Observed the Senior Operations Coordinator provision access to customer data to determine that customer data was restricted through the use of administrator groups.	No exceptions noted.
		Inspection: Inspected users with Super Administrator privileges and System Administrator privileges and their job responsibilities to determine that they were aligned with departments approved by management to have customer data access, and confirmed that customer data was restricted to authorized users based on their job function.	No exceptions noted.
7.3	Customer data is encrypted at rest using AES-256 encryption.	**Inquiry:** Inquired of the Senior Software Architect to determine that customer data was encrypted at rest using AES-256 encryption.	No exceptions noted.
		Inspection: Inspected the encryption configuration for the Google Cloud Platform managed by Workiva and the native encryption method used and managed by Amazon Web Services to determine customer data was encrypted using AES-256 encryption.	No exceptions noted.
		Inspection: Inspected a sample client's data within Google Cloud to determine that customer data was encrypted using AES-256 encryption.	No exceptions noted.

Control Objective 7

Controls provide reasonable assurance that data is appropriately secured and protected from unauthorized or unintentional use, modification, addition, or deletion.

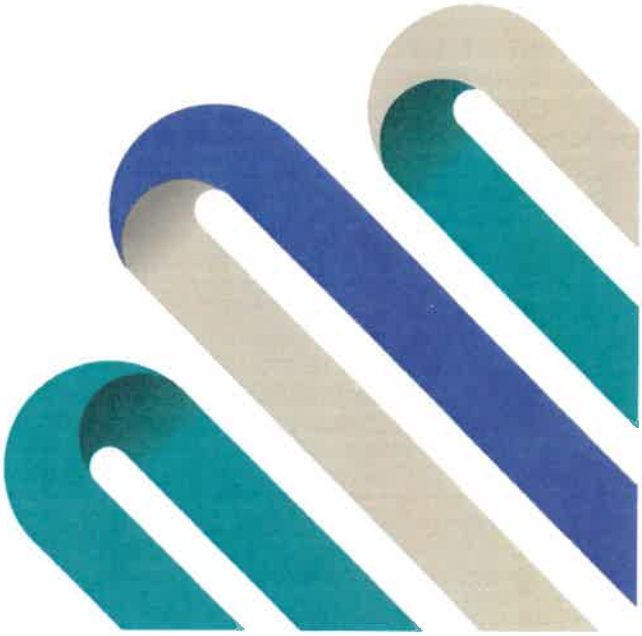
	Control Activity	Tests Performed By Service Auditor	Results of Testing
7.4	Devices of users with access to Restricted level data are encrypted in accordance with the requirements of the Encryption Standard.	**Inquiry:** Inquired of the Senior Director of Information Security to determine devices of users with access to Restricted-level data were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
		Inspection: Inspected the encryption settings for a sample of user devices with access to Restricted-level data to determine that the devices were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
7.5	Paper containing confidential information is destroyed by shredding or by placing in a designated shredding receptacle. Destruction is validated through the receipt of a certificate of destruction (tier I and II sites).	**Inquiry:** Inquired of the Chief Administration Officer to determine that paper containing confidential information was destroyed by shredding or by placing in a designated shredding receptacle and that destruction was validated through the receipt of a certificate of destruction.	No exceptions noted.
		Observation: Observed the shred bins throughout the headquarters to determine that shredding receptacles were made available to dispose of paper containing confidential information.	No exceptions noted.
		Inspection: Inspected the Information Asset Management Policy and the agreement with the shredding vendor to determine that a process and vendor were in place to destroy items disposed off in the shredding receptacle.	No exceptions noted.
		Inspection: Inspected the certificate of destruction for a sample of months to determine that destruction of confidential information placed in shredding receptacles was validated through the receipt of a certificate of destruction.	No exceptions noted.
7.6	Communication sessions between the Workiva product and user organizations are secured using TLS encryption	**Inquiry:** Inquired of the Senior Software Architect to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.
		Inspection: Inspected the digital certificate and encryption configuration for the Workiva product to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.

Workiva

WORKIVA, INC.

Cloud-Based Collaboration Solutions and Support Operations

System and Organization Controls (SOC) for Service Organizations Report
for the period of November 1, 2018 to October 31, 2019



Grant Thornton

Report of Independent Service Auditors issued by
Grant Thornton LLP

Contents

I. Report of Independent Service Auditors 1

II. Workiva, Inc.'s Assertion 5

III. Workiva, Inc.'s Description of its System and Controls 7

A. Overview of Services Provided 7

B. Principal Service Commitments and System Requirements 7

C. Components of the System Used to Provide the Services 7

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communications, and Monitoring 11

E. Changes to the System During the Specified Period 16

F. System Incidents 16

G. Additional Information about Management's Description 17

H. Subservice Organizations 17

I. User Entity Controls 19

IV. Description of the Trust Services Categories, Criteria, Workiva, Inc.'s Related Controls, and the Independent Service Auditor's Description of Tests and Results 22

A. Types and Descriptions of the Tests of Operating Effectiveness 22

B. Trust Services Categories, Criteria, Control Activities, and Testing Provided by the Service Auditor 23

V. Other Information Provided by Workiva, Inc. 237

A. HIPAA Mapping to SOC 2 Controls 237

GRANT THORNTON LLP
1201 Walnut Street, Suite 2200
Kansas City, MO 64106

D +1 816 412 2400
F +1 816 412 2404

I. Report of Independent Service Auditors

Board of Directors and Management
Workiva, Inc.

Scope

We have examined Workiva, Inc.'s (the "Company") accompanying description of its Cloud-Based Collaboration Solutions and Support Operations system titled "Workiva, Inc.'s Description of System and Controls" ("description") throughout the period November 1, 2018 to October 31, 2019 (the "specified period"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of the controls stated in the description throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

The information included in Section V of this report, "Other Information Provided by Workiva, Inc.," is presented by management of the Company to provide additional information and is not a part of the Company's description. Information about the Company's mapping of controls in this report relevant to certain Health Insurance Portability and Accountability Act of 1996 (HIPAA) requirements within the Security Rule and information about management's responses to testing exceptions has not been subjected to the procedures applied in the examination of the description and of the suitability of the design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria and, accordingly, we express no opinion on it.

The Company uses two subservice organizations, Google, LLC ("Google") and Amazon Web Services ("AWS"), to provide data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the

Grant Thornton

Company's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the Company's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service organization's responsibilities
The Company is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that the Company's service commitments and system requirements were achieved. The Company has provided the accompanying assertion titled "Workiva, Inc.'s Assertion" ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Company is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service auditor's responsibilities
Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and International Standard on Assurance Engagements (ISAE) 3000 (Revised), *Assurance Engagements Other than Audits or Reviews of Historical Financial Information*, issued by the International Auditing and Assurance Standards Board. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- obtaining an understanding of the system and the service organization's service commitments and system requirements;
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;

- testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent limitations
The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs.

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria.

Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of tests of controls
The specific controls tested and the nature, timing, and results of those tests are listed in Section IV of this report.

Opinion
In our opinion, in all material respects,

a. The description presents Workiva, Inc.'s Cloud-Based Collaboration Solutions and Support Operations system that was designed and implemented throughout the period November 1, 2018 to October 31, 2019, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that Workiva, Inc.'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 subservice organizations and user entities applied the complementary controls assumed in the design of Workiva, Inc.'s controls throughout the period November 1, 2018 to October 31, 2019.
c. The controls stated in the description operated effectively throughout the period November 1, 2018 to October 31, 2019, to provide reasonable assurance that Workiva, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Workiva, Inc.'s controls operated effectively throughout the period November 1, 2018 to October 31, 2019.

Grant Thornton

Restricted use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of the Company, user entities of the Company's Cloud-Based Collaboration Solutions and Support Operations system during some or all of the specified period, business partners of the Company subject to risks arising from interactions with the Cloud-Based Collaboration Solutions and Support Operations system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- the nature of the service provided by the service organization;
- how the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- internal control and its limitations;
- complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- user entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- the applicable trust services criteria; and
- the risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Grant Thornton LLP

Kansas City, MO
December 17, 2019

II. Workiva, Inc.'s Assertion

We have prepared the accompanying description of Workiva, Inc.'s (the "Company") Cloud-Based Collaboration Solutions and Support Operations system (the "System") titled "Workiva, Inc.'s Description of its Cloud-Based Collaboration Solutions and Support Operations" throughout the period November 1, 2018 to October 31, 2019 (the "specified period") (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) (description criteria). The description is intended to provide report users with information about the System that may be useful when assessing the risks arising from interactions with Workiva, Inc.'s system, particularly information about system controls that Workiva, Inc. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Workiva, Inc. uses two subservice organizations, Google, LLC ("Google") and Amazon Web Services ("AWS"), to provide data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Workiva, Inc., to achieve Workiva, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Workiva, Inc.'s controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Workiva, Inc.'s controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at Workiva, Inc., to achieve Workiva, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Workiva, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Workiva, Inc.'s controls.

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

A. The description presents the System that was designed and implemented throughout the specified period, in accordance with the description criteria.

B. The controls stated in the description were suitably designed throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the specified period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of the Company's controls throughout the specified period.

C. The controls stated in the description operated effectively throughout the specified period to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization(s) and complementary user entity controls assumed in the design of the Company's controls operated effectively throughout the specified period.

III. Workiva, Inc.'s Description of its System and Controls

A. Overview of Services Provided

Workiva (NYSE:WK) delivers Wdesk, an intuitive cloud platform that modernizes how people work within thousands of organizations, including over 75 percent of the 500 largest U.S. corporations by total revenue. Wdesk is built upon a data management engine, offering controlled collaboration, data connections, granular permissions, and a full audit trail. Wdesk helps mitigate risk, improves productivity, and gives users confidence in their data-driven decisions. For more information, visit workiva.com.

Wdesk is available as a subscription service. The company also offers customers support and professional services. Wdesk was created by experienced accountants, engineers, and entrepreneurs dedicated to helping public and private companies reduce time, risk, and costs associated with business reporting.

Occasionally, Workiva may make features or products available to select customers under a "Beta" or "Customer Development Program" agreement. These are not in scope for this report and would be addressed by a separate customer agreement, as appropriate.

B. Principal Service Commitments and System Requirements

Workiva designs its processes and procedures to meet its objectives for its services based on the commitments that Workiva makes to its customers, the laws and regulations that govern the provision of services, and the financial, operational, and compliance requirements that Workiva has established for the services. In addition, the security infrastructure of Workiva's services are mapped to the security and privacy requirements of the Health Insurance Portability and Accountability Act, as amended.

Workiva establishes information security policies that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system operates, how the internal business systems and networks are managed and how employees are hired and trained.

Security commitments to Workiva's customers are documented and communicated in a variety of ways including, in Workiva system policies and procedures, via its standard form customer agreements, by responding to customer questionnaires, or through the provision of CAIQs.

C. Components of the System Used to Provide the Services

1. Infrastructure

The Workiva Platform runs in both Google Cloud and Amazon Web Services (AWS).

The Workiva Platform uses Google Application Engine and Google Compute engine for front-end and preliminary application workloads. AWS services are utilized for microservices and backend services processing. AWS Elastic Kubernetes Service provides the environment for microservices orchestration and AWS Elastic Compute service provide the resources backend services processing for non-microservices application processing.

Communication between Workiva Platform services is secured in-transit with TLS 1.1 or better and data is encrypted with AES-256 encryption at rest.

Amazon Aurora 2 database services are utilized for data persistence. Communications to and from the data layer are secured in transit with TLS 1.1 or better and data at rest is encrypted with AES-256.

2. Software

Wdesk is a web application developed and maintained by Workiva's in-house research and development group. This R&D group enhances and maintains Wdesk to provide reporting and collaboration services for the company's customers. Wdesk is sold directly to customer organizations or their finance/accounting departments.

Wdesk tracks changes to customer documents in real time. The information is immediately stored in a data persistence layer consisting of Google Cloud Storage DataStore, Amazon Web Services Simple Cloud Storage Service (AWS S3) and Amazon Web Services Relational Database Service (AWS RDS).

Wdesk's interface is a Software as a Service (SaaS) multiuser web application that manages, secures and provides reliable access to customer financial documents. Individual software microservices provide discrete functionality for the SaaS application in a highly available fashion.

3. People

Workiva has a staff of more than 1,400 employees organized in the following functional departments:

- Research and Development, Infrastructure and Reliability Engineering. These teams are responsible for the broad range of software systems development and application support, including testing and ensuring the integrity of the Workiva platform.

- Customer Success. Customer Success is available to Workiva users, 24 hours a day, 7 days a week, 365 days a year. Responsibilities include working on customer support tasks, responding to customer questions, incidents, and service requests, and notifying customers of upcoming changes. In addition, the Customer Success team ensures that any system interruptions are detected instantly; oversees day-to-day support activity; and directs customer onboarding, which includes analysis and implementation of financial reporting documents and templates within Wdesk, end-user training, and the transition to the dedicated Customer Success Manager.

- Professional Services. Professional Services helps customers experience manage discrete aspects of their reporting within the Workiva platform, including a variety of XBRL® and taxonomy support options to assist with tagging and best practices

- Information Security. This team includes help desk, IT infrastructure, IT networking, IT system administration, software systems development and application support, information security, and IT operations personnel manage electronic interfaces and business implementation support and telecom. The information security staff supports Workiva platform indirectly by monitoring internal and external security threats and maintaining current antivirus software, maintaining the inventory of IT assets, and providing infrastructure support as well as disaster recovery assistance.

- Corporate. The Corporate team includes executives, senior operations staff, and company administrative support staff, such as sales, accounting, finance, legal, compliance, internal audit, information technology, training, human resources, marketing, public relations. These individuals use the Workiva platform primarily as a tool for internal metrics, presentations, and content and document management.

4. Data

Workiva encrypts all customer data before it is stored using the AES 256 encryption algorithm.

When the encrypted customer data is written to the Google App Engine Datastore, the underlying Google File System logic shards the data and distributes it across multiple physical and virtual servers for optimal data retrieval. An individual customer's data is distributed among multiple physical and virtual servers. Redundancy is achieved by writing data in parallel to multiple datacenters in different geographic locations. Failure or high latency of one data location causes the Google File System to failover to another location that might be in a different datacenter.

Similarly, when the encrypted customer data is written to the Amazon Web Services platform, the underlying redundancy logic helps ensure that copies are available across availability zones. Failure or high latency of one data location causes service to failover to another location that might be in a different availability zone.

Wdesk services run in a restricted sandbox environment within both Google App Engine (GAE) and Amazon Web Services (AWS), and this environment enforces separation between cloud tenants as well as a number of security-related controls.

Regardless of data storage location, all customer data, in transit and at rest, is subjected to Workiva's encryption and key management standards. In the Amazon Web Services environment, Workiva makes use of the supplied Key Management Service to fully encrypt databases or drives that contain customer information. Identity and Access Management (IAM) profiles are used to ensure appropriate restriction of access to the keys and data they secure.

Wdesk access is controlled through Workiva's authentication and authorization system. This system allows customers to set custom password requirements and login timeouts (default of one hour) as an administrative function. Customers may set password expiry rules and force individual users or all users to reset their passwords. Two-factor authentication (PIN + rotating authentication code) and Single Sign-on (SAML 2.0) are available as optional features.

Plain-text passwords are never stored within the Google App Engine datastore. Workiva stores a salted hash of the user's password to resist pre-computation attacks. Additionally, hashing is performed in a way that resists brute-force attacks (computationally intensive hashing with several thousands of rounds).

Workiva's authentication system also includes an optional lockout policy that subsequently requires an account administrator to unlock an account after a defined number of attempts. If this option isn't selected, accounts are locked out for an exponentially increasing amount of time, up to 15 minutes, on subsequent invalid login attempts. Customers may choose to lockout individual users or deny access to all accounts.

Wdesk features a permissions system that customers use to control access to documents, sections, and other content displayed in the editor and reader. Coupled with Workiva's authentication system, the permissions system governs the data accessible by the end-user.

Initiation of each new Workiva customer follows a detailed process to provide assurance that only authorized individuals are provided with access to the application. Additional changes made by Workiva personnel are logged, tracked, and follow the same authorization process. Customer administrative changes are tracked within the application providing self-audit capabilities.

Workiva maintains an up-to-date record of all tagged, data-bearing Workiva owned IT assets. This record includes the owner (person), department, location, unique identifier, purchase date, model,

and value. Assets without an owner assigned are prohibited from use. Policies and procedures are in place for the sanitization of equipment that has stored non-public information prior to re-use. Equipment that has stored non-public information is sanitized in accordance with Workiva's Information Classification Standard before it can be disposed of.

5. Policies and Procedures

Workiva implements a number of internal policies and procedures to help ensure that customer information is kept confidential and secure. Corporate governance policies and agreements include the following:

- Information Security Program Charter
- Application Development Security Policy
- Business Continuity Policy
- Change Management Policy
- Customer Data Access Policy
- Encryption Policy
- Endpoint Device Security Policy
- Identity & Access Management Security Policy
- Incident Management Policy
- Information Classification Standard
- Information Assessment Management Policy
- Personnel Security Policy
- Physical Security Policy
- Risk Management Policy
- Security Assessment Policy
- Server & Network Device Security Policy
- Third-Party Relationships Security Policy
- Internal IT and Wdesk Procedures
- Third-Party Non-Disclosure Agreement
- Third-Party Security Standard Consultant Agreement
- Customer Confidentiality and Securities Trading Policy
- WLife Employee Handbook (including portions of the above).

Workiva maintains these policy and procedure documents for at least six years. Policies are included in WLife, and available on the company intranet. Procedures are published on the company intranet.

D. Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communications, and Monitoring

The security category and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in section 4 of this report. Although the applicable trust services criteria and related controls are included in section 4, they are an integral part of Workiva, Inc.'s description of the Cloud-Based Collaboration Solutions and Support Operations system.

1. Control Environment

Management Philosophy

The control environment at Workiva is process-based, situated within an organizational structure designed to optimize the delivery of services to all customers. Executive and senior leadership provide governance and play an integral role in establishing the core values and culture of the organization. The Chief Compliance Officer provides leadership and oversight of controls and security to execute the governing principals set forth by the Executive Management team. This role also provides for the auditing of processes and controls, actively reviewing key areas on a continual basis.

Functional departments engage each employee in the controls process, providing an environment that facilitates a flow of knowledge, empowers execution, and ensures a clear understanding of responsibilities and obligations. Core production departments include Research and Development, Infrastructure and Reliability, Customer Success, and Professional Services. Supporting departments include Corporate Marketing, Human Asset Management, Accounting, Finance, Corporate Administration, Information Technology, Quality Assurance, and Sales.

Security Management

Workiva maintains an Information Security program designed to protect the security, confidentiality, integrity, availability, and privacy of its computing infrastructure and associated customer confidential data. It is the policy of Workiva to establish management direction and define procedural requirements for Information Security to help ensure the appropriate protection of information and assets of the organization and its customers in a manner commensurate with its confidentiality, value, and criticality while also meeting regulatory requirements. Workiva therefore utilizes a policy-driven information security architecture approach that is coordinated and managed by the Information Technology department and integrated into the Information Security risk management process. Implementation and execution is further facilitated through cross-functional groups brought together to address key requirements. Workiva Information Security policies are reviewed and approved by management, and received and signed by all employees.

Information security at Workiva is a team effort, involving the participation and support of every employee. This program includes:

- Provisions for the education of employees on information security awareness
- Establishment, assessment, and maintenance of policies and procedures
- Investigation of suspected abuses of Workiva information systems, information, and communication mediums
- A functional and clearly communicated Incident Management Standard.

Personnel Security

Workiva employee and consultant hiring procedures include background checks. Termination procedures ensure return and/or destruction of any and all company and customer information and suspension of access to company networks and software systems. In addition, termination of technical and customer support personnel may require additional action including account suspension for enterprise software systems for which they may have administrative access.

Workiva Human Asset Management team relies upon a clearly defined hiring process that includes the following steps:

- Initiate recruiting efforts as necessary
- Complete pre-screening of resumes
- Select interview candidates
- Set up and conduct interviews
- Make final candidate selection
- Request authorization to complete background checks and check references
- Check references
- Complete background checks
- Make written employment offer
- Upon receiving signed offer letter, prepare all remaining employment documents, including Confidentiality and Inventions Assignment Agreement and I9 Form

On employee's first day of work, employee is provided an orientation session that includes an Information Security session given by a member of the Information Security team and is given access to WLife (a compilation of corporate policies) and Customer Confidentiality and Securities Trading Policy. Employees are asked to sign and acknowledge receipt and compliance with these documents.

Recurring training occurs throughout the year, specifically making sure that personnel are trained on security awareness and trading compliance annually. Employees review the code of conduct and acknowledge receipt to be in compliance with WLife on an annual basis. Users with elevated levels of access undergo additional training that address specific Security and Confidentiality requirements in relation to their job functions on an annual basis.

Physical Security and Environmental Controls

Workiva offices are secured with a proximity badge system and are monitored with a system of high-resolution IP cameras. This security system controls access to non-public entrances, private areas, and restricted areas at all times and public entrances outside of business hours. Footage is captured 24/7, and is retained for 90 days. All facilities are equipped with shred bins and employees are trained to shred all paper containing even potentially confidential information.

Public entrances are staffed and monitored by a receptionist who manages a visitor sign-in log, ensures visitors complete a non-disclosure agreement, and issues visitor badges. Employees badge in and out at all entrances, and the times are recorded. Access to offices is maintained in conjunction with the Human Asset Management change process, and management performs a comprehensive access review annually.

Workiva performs a risk assessment of vendors' security and capabilities. This review is conducted commensurate with the level of information they have access to.

Change Management

Workiva uses a defined Software Development Life Cycle (SDLC) with an emphasis on functionality, quality, responsiveness, and security. This systematic approach includes a process to ensure that any changes to systems or applications are thoroughly reviewed, tested, approved, and well communicated.

The SDLC employs Agile software development practices designed to be nimble and responsive with customers and the market. Research & Development teams prioritize their work and maintain a queue of work that is planned and in-progress. Teams meet regularly to review their work with the larger organization, hold planning meetings, and hold retrospectives to review how they are working as a team and identify performance improvements going forward. Many teams also hold stakeholder meetings where they invite stakeholders to provide input on their future direction.

Updates to Wdesk are released on a regular basis as work is completed. Release Management verifies completion of all SDLC requirements for any code before it is used in the production environment.

Members of Research & Development, Information Technology, Infrastructure & Reliability, Quality Assurance, and Information Security with knowledge and training in software and Information Security are authorized as Security Reviewers. These individuals are involved in all phases of product development, and review changes to software code that is security-sensitive. This includes code involved in session management, access control, APIs that perform cross-platform calls, authentication, input validation, output encoding, secure transmission, audit logging, file uploads, XSS/CSRF protection, or encryption/hashing. Additions and modifications to this code are consistently reviewed and approved by authorized reviewers prior to being merged into the master codebase. An automated monitoring system, built and maintained by the Information Security team, is in place to help ensure items are appropriately flagged for security review. In addition, great care is taken during the design and prototyping phases of any feature set to identify architecture and implementation that may require security consideration. New feature sets requiring security consideration are subject to a full Information Security team assessment prior to production release.

Workiva leverages a combination of software development tools and a defined process to facilitate the flow, structure, communication, collaboration, and management of product development. Examples of this integration of tools and process include:

- Segregated development, testing, and production environments that are maintained for the security and integrity of the system.
- Project management tools and ticketing system that provide tracking of all projects from initiation to implementation. Work is tracked in order to provide a clear path for all team members, and a mechanism to adjust project parameters and requirements.
- Advanced automated and/or manual quality assurance testing tools that are used to maximize the operating capabilities of Wdesk.
- Development items that have security impact are identified and tracked in the project management/ticketing system. This allows issues/changes that have a potential security impact to be easily identified, and routed for code review, security review, and receive final sign-off by the Information Security team prior to release into production.
- The project management/ticketing system provides the functionality necessary to achieve and record all required management sign-offs prior to any code releases.

- Version control software used to manage current versions of source code for the in-scope applications. The ability to modify source code for the in-scope applications is restricted to appropriate personnel based on job function.

System Monitoring

Internally, Workiva utilizes both automated and periodic manual review systems to provide a high level of service and availability. Customers are provided with proactive monitoring tools within the Wdesk environment to review key activities, such as authentication, authorization, permissions, and document changes. Workiva and its partners use a combination of commercially available tools and custom tools to detect suspicious activity.

Examples of monitoring activities in each of these categories include:

Internal

- Logging and monitoring of SEC filing activities
- Application operating parameters and performance
- Application operation transaction exceptions
- System administration authentication and activity
- Application development activities and production changes
- Security incidents and security related development activities
- Application access reviews
- Regular internal audits and vulnerability assessments
- Periodic third-party security vulnerability assessments
- System log analysis review

Customer

- Authentication activities
- Application access reviews
- User additions
- Permissions and authorization changes
- Document change history
- User role changes

Data Backup and Recovery

Production environments are backed up in full at least weekly and the backup files are encrypted. Backup software is configured to alert IT personnel for any backup failure, which is resolved appropriately. Access to the backup tool is restricted to members of the infrastructure team. Data restore testing of backup files is performed at least annually.

System Account Management

Workiva defines acceptable channels through which restricted-level customer data can be transferred that adhere to the security and confidentiality obligations and trains employees on these channels. Access to systems that contain restricted level customer data requires users to authenticate via a single sign-on system. System administration tasks require the use of a multi-factor authenticated VPN to access consoles.

Production systems conform to documented configuration hardening guidelines, including firewall rules. These systems are audited for conformance with the hardening guidelines on a weekly basis with the use of automated scans. Firewalls rules are reviewed for appropriateness and approved by management on a semi-annual basis.

The granting or modification of access rights is based on the concept of least privilege and must be authorized and approved by the user's functional manager and the application owner. Approvals are requested, tracked, and resolved by workflow management tools. Administrative production system access is granted only to individuals who have been trained and require this level of access to perform required tasks. Access to production systems is removed by the system owner upon submission of a termination request by Human Asset Management. Users are required to utilize unique user IDs to access systems. Passwords adhere to the documented password policy, including complexity, length, re-use restrictions, and expiration requirements. Access to systems containing Restricted information makes use of two-factor authentication for Workiva personnel. User access is reviewed and certified by management on a semi-annual basis.

Customer user account management requests must be appropriately authorized per customer agreement.

2. Risk Assessment Process

Workiva management understands the benefits of proactive risk management and maintains a formal risk management program. This program relies on input from business units, support resources, and executive management to identify, assess, and mitigate risk across the business. Core functional departments, such as Research & Development and Customer Success, identify and report situations where risk levels are outside of established organizational tolerance levels. The Information Security team takes a proactive approach and conducts audits and assessments to ensure controls are adequate and operating as designed.

The Workiva control environment is subject to internal and external assessments. The Workiva Information Security team maintains a framework to facilitate risk review and validation using internal testing as well as vulnerability assessments by third parties. The team reviews all security-related issues during product development and prior to deployment, and works to develop, review, and disseminate Information Security-related policies, standards, and procedures.

Workiva has an established Incident Management Standard that outlines communication and escalation in the event of any type of event outside of normal business operations.

3. Information and Communication Systems

Workiva applies various communication strategies, both internal and customer facing, to ensure that information is effectively distributed, available, and used in implementing and executing actions to achieve organizational goals, as well as delivering expected value to customers.

Internal

Workiva utilizes several mechanisms to communicate information across the organization. Several of the key tenets of communication within the organization encourage content to be timely, relevant, clear, complete, and appropriate. An intranet is used to communicate general information to employees, including policies, procedures, and general business updates. Additional tools include email, new hire orientation, training, regular management meetings, and video broadcasts. Any product service interruptions or changes are promptly communicated internally between departments according to the Incident Management Standard, and depending upon impact to the customer experience, communicated directly to impacted parties.

External

The Customer Success department provides the primary direct communication interface for Workiva customers. Telephone, email, and cell phone provide direct access for customers to contact Workiva with any inquiry. Proactive communications are also initiated to alert customers of

incidents or significant changes to the application or operating environment. Customers are also provided a mechanism via Wdesk to request enhancements and provide feedback.

4. **Monitoring Controls**

Workiva recognizes the need to be alert to external risks and vigilant in looking for potential issues or active incidents. Workiva evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its ongoing risk assessment and management process and revises these when necessary to meet changing commitments and requirements. System architecture diagrams depicting details of production systems and the system boundary are maintained for use in describing and auditing the Wdesk environment.

Workiva performs the following incident and risk management activities on an annual basis:

- Conducts a risk assessment and business impact analysis to evaluate risks to the Wdesk environment and to ensure the appropriateness of controls.
- Performs a business continuity exercise that includes both technical and pandemic scenarios.
- Trains members of the Incident Response Team to ensure awareness of proper escalation paths and criteria.

The Incident Management Standard addresses identification, documentation, resolution, communication, and escalation of both operational and security incidents. Active monitoring provides key information used to identify potential incidents. Management monitors employees' compliance with the code of conduct through monitoring of customer and employee complaints and the use of an anonymous third-party administered ethics hotline. Workiva policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct. Monitoring software is used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes and alert operations personnel for remediation.

Proactive third-party vulnerability assessments are performed semi-annually and internal assessments are performed monthly on Workiva applications to identify additional potential exposures. Additionally, internal reviews of compliance with information security policies are performed on a monthly basis. Internal testing and in-house tools are also used as a component of the quality assurance process to maximize identification of potential risks.

This proactive stance applies to all aspects of the Workiva infrastructure. Anti-malware programs are installed on all company-issued laptops. All devices for users with access to Restricted data are encrypted and prevented from writing to removable media and these users are required to use their Workiva device when handling Restricted data. Workiva works closely with its vendors to help ensure they have equally stringent Incident and Risk Management programs in place. Vendors providing mission-critical services in support of the production environment are reviewed annually by Workiva to identify both capability and risk. A mission critical service is defined as one that requires continuous availability. Breaks in service are intolerable and immediately and significantly damaging. Agreements with sub-processors of restricted-level customer information include language to address security and confidentiality requirements.

E. Changes to the System During the Specified Period

There were no changes that are likely to affect report users' understanding of how the Cloud-Based Collaboration Solutions and Support Operations system is used to provide the service during the period from November 1, 2018, through October 31, 2019.

F. System Incidents

Workiva, Inc. did not encounter any incidents that (a) were the result of controls that were not suitably designed or operating effectively or (b) otherwise resulted in a significant failure in the achievement of

one or more of those service commitments and system requirements during the period of time covered by the description

G. Additional Information about Management's Description

The controls supporting the service organization's service commitments and system requirements based on the applicable trust services criteria are included within Section IV of this report, "Description of the Trust Services Categories, Criteria, Workiva, Inc.'s Related Controls, and the Independent Service Auditor's Description of Tests and Results." Although the applicable trust services criteria and related control activities are presented within Section IV, they are an integral part of the Company's description of its system.

H. Subservice Organizations

The Company utilizes subservice organizations to perform certain functions. The description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at the third-party service organizations described below. The examination by the Independent Service Auditor did not extend to the policies and procedures at these subservice organizations.

Complementary subservice organization controls, controls that management of the service organization assumes will be implemented by the subservice organization and are necessary to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria, along with the associated subservice organizations, are included within the table below. Management also describes the activities performed to monitor the effectiveness of controls at the subservice organization. Each user entity's internal control must be evaluated in conjunction with the Company's controls and the related tests and results described in Section IV of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Google LLC ("Google")	The Company uses Google for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications; and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following controls to help monitor the subservice organization: • An annual risk assessment review is conducted of vendors providing mission critical services in support of the production environment; and • Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	CC 5.5*

Subservice Organization	Services Provided/Complementary Controls/Monitoring Controls	Associated Criteria
Amazon Web Services ("AWS")	The Company uses Amazon Web Services for its third-party hosting of servers and equipment, including the restriction of physical access to the defined system including, but not limited to, facilities, backup media, and other system components such as firewalls, routers, and servers. The following control areas are critical to achieving the Company's service commitments and system requirements based on the applicable trust services criteria: • Controls around the physical security of the Data Centers hosting the in-scope applications, and • Controls, including environmental controls, around the backup processes at the Data Centers hosting the in-scope applications to support the disaster recovery processes. In addition, the Company has identified the following controls to help monitor the subservice organization: • An annual risk assessment review is conducted of vendors providing mission critical services in support of the production environment; and • Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment	CC 5.5*, CC 7.4*

* The achievement of design and operating effectiveness related to this criterion assumes that the complementary controls at this subservice organization that support the service organization's service commitments and system requirements are in place and are operating effectively.

I. User Entity Controls

Workiva, Inc.'s controls relating to the system cover only a portion of the overall internal control structure of each user entity of the Company. It is not feasible for the Company's service commitments and system requirements to be achieved based on the applicable trust services criteria solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related testing detailed in Section IV of this report, taking into account the related complementary user entity controls identified within the table below, where applicable. Complementary user entity controls and their associated criteria are included within the table below.

Management has highlighted criterion in which complementary user entity controls were assumed in the design of the Company's system with an asterisk. In order for user entities to rely on the controls reported on herein, each user entity must evaluate its own internal control environment to determine if the identified complementary user entity controls have been implemented and are operating effectively.

Furthermore, the table below includes suggested control considerations that the Company believes each user organization should consider in developing their internal controls or planning their audits that are relevant to the Company's controls detailed in this report, however, such control considerations are not required to achieve design or operating effectiveness for the Company's service commitments and system requirements based on the applicable trust services criteria. The following list of suggested control activities is intended to address only those policies and procedures surrounding the interface and communication between the Company and each user entity. Accordingly, this list does not allege to be, and is not, a complete listing of all the control activities which provide a basis for the assertions underlying the control environments for the Company's user entities.

User Entity Control	Associated Criteria
Customers are responsible for completeness, accuracy, and timeliness of the information that is created, manipulated, and filed in the process of using Wdesk.	CC 5.2*, CC 6.1*
Customers are responsible for administering and monitoring all user accounts with access to their data.	CC 5.2*, CC 6.1*
Customers are responsible for the logical security of all devices involved in the use of Wdesk that are used by customers or agents of the customer.	CC 5.2*, CC 6.1*
Customers are responsible for establishing and enforcing their own password security policy and enabling appropriate controls in Wdesk.	CC 5.2*, CC 6.1*
Customers are responsible for setting and maintaining document permissions on a per-section basis for editing and reading.	CC 5.2*, CC 6.1*
Customers are responsible for security and reliability of the connection to Wdesk.	CC 6.7
Customers are responsible for Information Security training for all users with access to their data.	CC 5.2*, CC 6.1*
Customers are responsible for contacting and working cooperatively with Workiva if there are any issues with security including, but not limited to, unauthorized use of their password or account	CC 5.2*, CC 6.1*, CC 7.3*, CC 7.4*
Customers are responsible for backing up data in accordance with their own relevant requirements.	CC 9.1*
Customers are responsible for the physical security of all devices involved in the use of Wdesk that are used by customers or agents of the customer.	CC 6.4*
Customers are responsible for specifying one or more administrators who will have the appropriate rights and permissions to access the administrative tools provided with Wdesk.	CC 5.2*, CC 6.1*
Customers are responsible for maintaining and communicating to Workiva the accurate Account Administrator contact information for all designated account administrators.	CC 5.2*, CC 6.1*

User Entity Control	Associated Criteria
Customers are expected to self-administer the desired level of document retention by backing up their critical data using the tools provided within Wdesk.	C 1.2

* The achievement of design and operating effectiveness related to this criterion assumes that the complementary user entity controls that support the service organization's service commitments and system requirements are in place and are operating effectively.

IV. Description of the Trust Services Categories, Criteria, Workiva, Inc.'s Related Controls, and the Independent Service Auditor's Description of Tests and Results

A. Types and Descriptions of the Tests of Operating Effectiveness

This report, when combined with an understanding of the controls at user entities and subservice organizations, is intended to provide user entities of the Company's System, those prospective user entities, practitioners providing services to such user entities, and other specified parties with information about the control features of the Company's System. The description is intended to provide users with information about the System. Our examination was limited to the applicable trust services criteria and related controls specified by the Company in sections III and IV of the report and did not extend to the controls in effect at user entities and subservice organizations. It is the responsibility of each specified party to evaluate this information in relation to the control structure in place at the user organization to assess the total internal control environment. If internal control is not effective at user entities, the Company's controls may not compensate for such weaknesses.

The Company's system of internal control represents the collective effect of various factors on establishing or enhancing the effectiveness of the controls specified by the Company. In planning the nature, timing, and extent of our testing of the controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, we considered aspects of the Company's control environment, risk assessment process, monitoring activities, and information and communications.

The following table clarifies certain terms used in this section to describe the nature of the tests performed:

Type	Description
Inquiry	Inquired of appropriate personnel and corroborated with management
Observation	Observed the application, performance, or existence of the control
Inspection	Inspected documents, records, or other evidence indicating performance of the control

In addition, when using information produced (or provided by) the service organization, we evaluated whether the information was sufficiently reliable for our purposes by obtaining evidence about the accuracy and completeness of such information and evaluating whether the information was sufficiently precise and detailed for our purposes.

B. Trust Services Categories, Criteria, Control Activities, and Testing Provided by the Service Auditor

Workiva establishes information security policies that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Information security policies define an organization-wide approach to how systems and data is protected. These include policies around how the service is designed and developed, how the system operates, how the internal business systems and networks are managed and how employees are hired and trained.

Security commitments to Workiva's customers are documented and communicated in a variety of ways including, in Workiva system policies and procedures, via its standard form customer agreements, by responding to customer questionnaires, or through the provision of CAIQs.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	CC 1.1-01	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
				Inspection: Inspected the written job description and the HR job offer workflow for a sample of job positions to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
		CC 1.1-02	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and if required, updates were made.	No exceptions noted.
		CC 1.1-03	Performance reviews are conducted at least annually for employees within the Information Security team.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that performance reviews were conducted at least annually for employees within the Information Security team.	No exceptions noted.
				Inspection: Inspected the most recent annual performance review for a sample of employees within the Information Security team to determine that performance reviews were conducted at least annually for these employees.	No exceptions noted.
		CC 1.1-04	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			entities, and compliance.	organizational entities, and compliance.	
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 1.1-05	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.	**Inquiry**: Inquired of the VP of HR to determine that personnel were required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.
				Inspection: Inspected the signed copy of the Code of Conduct for a sample of new and current employees to determine that personnel were required to read and accept the Code of Conduct, which included the statement of confidentiality and privacy practices, upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 1.1-06	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.
		CC 1.1-07	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 1.1-08	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 1.1-09	The head of the Internal Audit function reports to the Audit Committee of the Board of Directors functionally and administratively.	**Inquiry**: Inquired of the Director of Information Security to determine that the head of the Internal Audit function reports to the Audit Committee of the Board of Director functionally and administratively.	No exceptions noted.
				Inspection: Inspected the Audit Committee Charter to determine that the head of the Internal Audit function reports to the Audit Committee of the Board of Directors functionally and administratively.	No exceptions noted.
		CC 1.1-10	Enforcement of Workiva's Information Security policy is the responsibility of a Chief Compliance Officer or delegate.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that enforcement of Workiva's Information Security Policy was the	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				responsibility of a Chief Compliance Officer or delegate.	
		CC 1.1-11	Documentation of internal processes, policies and procedures is available on the Workiva intranet and retained for at least 6 years.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that processes, policies and procedures were documented and published on the Company intranet.	No exceptions noted.
				Inspection: Inspected the storage location of processes, policies and procedures to determine that they were available on the Company intranet.	No exceptions noted.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	CC 1.2-01	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	**Inquiry**: Inquired of the VP of Human Resources to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revised them when necessary to help meet changing commitments and requirements.	No exceptions noted.
				Inspection: Inspected the reporting lines in the HR system for a sample of employees to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected an email announcement from management about the realignment of organizational personnel under new leadership to determine that the entity evaluated its organizational structure, reporting lines, authorities, as changes occurred in the organization.	No exceptions noted.
		CC 1.2-02	Workiva's Board of Directors has established an Audit Committee to oversee the Internal Audit function directly.	**Inquiry**: Inquired of the Director of Information Security to determine that Workiva's Board of Directors had established an Audit Committee to oversee the Internal Audit function directly.	No exceptions noted.
				Inspection: Inspected the Audit Committee Charter to determine that Workiva's Board of Directors had established an Audit Committee to oversee the Internal Audit function directly.	No exceptions noted.
				Inspection: Inspected the meeting minutes from the most recent meeting of the Audit Committee meeting to determine that an Audit Committee existed and met quarterly to provide oversight of the Internal Audit function directly.	No exceptions noted.
		CC 1.2-03	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				employees and their supervisors.	
				Inspection: Inspected the written job description and the HR job offer workflow for a sample of job positions to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
		CC 1.2-04	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and and if required, updates were made.	No exceptions noted.
		CC 1.2-05	The head of the Internal Audit function reports to the Audit Committee of the Board of Directors functionally and administratively.	**Inquiry**: Inquired of the Director of Information Security to determine that the head of the Internal Audit function reports to the Audit Committee of the Board of Director functionally and administratively.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Audit Committee Charter to determine that the head of the Internal Audit function reports to the Audit Committee of the Board of Directors functionally and administratively.	No exceptions noted.
CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	CC 1.3-01	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 1.3-02	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
		CC 1.3-03	A Data Classification policy is in place and defines handling procedures for each level of classification.	**Inquiry**: Inquired of the Director of Information Security to determine that a Data Classification policy was in place and defined handling procedures for each level of classification.	No exceptions noted.
				Inspection: Inspected the Data Classification Policy to determine that a policy was in place and defined handling procedures for each level of classification.	No exceptions noted.
		CC 1.3-04	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
				Inspection: Inspected the written job description and the HR job offer workflow for a sample of job positions to determine that roles and responsibilities were defined in written job descriptions and	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				communicated to employees and their supervisors.	
		CC 1.3-05	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and and if required, updates were made.	No exceptions noted.
		CC 1.3-06	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 1.3-07	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.	**Inquiry**: Inquired of the VP of HR to determine that personnel were required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.
				Inspection: Inspected the signed copy of the Code of Conduct for a sample of new and current employees to determine that personnel were required to read and accept the Code of Conduct, which included the statement of confidentiality and privacy practices, upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 1.3-08	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.
		CC 1.3-09	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 1.3-10	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 1.3-11	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	**Inquiry**: Inquired of the VP of Human Resources to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revised them when necessary to help meet changing commitments and requirements.	No exceptions noted.
				Inspection: Inspected the reporting lines in the HR system for a sample of employees to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.
				Inspection: Inspected an email announcement from management about the realignment of organizational personnel under new leadership to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				determine that the entity evaluated its organizational structure, reporting lines, authorities, as changes occurred in the organization.	
		CC 1.3-12	Enforcement of Workiva's Information Security policy is the responsibility of a Chief Compliance Officer or delegate.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
		CC 1.3-13	Documentation of internal processes, policies and procedures is available on the Workiva intranet and retained for at least 6 years.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that processes, policies and procedures were documented and published on the Company intranet.	No exceptions noted.
				Inspection: Inspected the storage location of processes, policies and procedures to determine that they were available on the Company intranet.	No exceptions noted.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain	CC 1.4-01	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading	**Inquiry**: Inquired of the VP of HR to determine that employees were trained on Security Awareness and the Customer Confidentiality	No exceptions noted

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
	competent individuals in alignment with objectives.		Policy upon hire and annually.	and Securities Trading Policy upon hire and annually.	
				Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
		CC 1.4-02	The Information Security team distributes security-related education and awareness communications to employees on a quarterly basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.
				Inspection: Inspected the Information Security communication for a sample of quarters to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.
		CC 1.4-03	The organization maintains and publishes a Restricted Trade List and a policy is in place to prohibit employees from engaging in insider	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			trading. An intent-to-trade process exists to allow employees to request permission to conduct trading activities.	**Inspection**: Inspected the Restricted Trade List/No Trade List to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
				Inspection: Inspected the script used to automatically update the Restricted Trade List to determine that the organization had a process to scan for and identify new accounts to add to the Restricted Trade List based on newly onboarded clients.	No exceptions noted.
				Inspection: Inspected the Insider Trading Policy to determine that a policy was in place to prohibit employees from engaging in insider trading and defined a process to allow employees to request permission to conduct trading activities.	No exceptions noted.
		CC 1.4-04	Employees with access to system administration and diagnostic tools for production systems complete annual training specific to the risks and obligations of their access.	**Inquiry**: Inquired of Senior Director of Information Security to determine that employees with access to system administration and diagnostic tools for production systems completed annual training specific to the risks and obligations of their access.	No exceptions noted.
				Inspection: Inspected the training completion results for a sample of employees with access to system administration and diagnostic tools to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				determine that they completed annual training specific to the risks and obligations of their access.	
				Inspection: Inspected the Being a Wdesk Administrator training to determine that its content included information specific to the risks and obligations of the employees with access to system administration and diagnostic tools for production systems.	No exceptions noted.
		CC 1.4-05	The organization performs a background check on individuals as a component of the hiring process, as permissible in each country, and will decline to hire any individual with a felony conviction, or a conviction for theft or fraud. Workiva will review convictions for misdemeanors to determine whether they would compromise safety or security.	**Inquiry**: Inquired of the VP of HR to determine that the entity performed background checks on individuals as a component of the hiring process, as permissible in each country, and declined to hire any individual with a felony conviction, or a conviction for theft or fraud. In addition, the company reviewed convictions for misdemeanors to determine whether they would compromise safety or security.	No exceptions noted.
				Inspection: Inspected the background check report for a sample of new hires to determine that the entity performed background checks on individuals as a component of the hiring process, as permissible in each country, and will decline to hire any individual with a felony conviction, or a	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				conviction for theft or fraud.	
		CC 1.4-06	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
				Inspection: Inspected the written job description and the HR job offer workflow for a sample of job positions to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
		CC 1.4-07	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and and if required, updates were made.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 1.4-08	Performance reviews are conducted at least annually for employees within the Information Security team.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that performance reviews were conducted at least annually for employees within the Information Security team.	No exceptions noted.
				Inspection: Inspected the most recent annual performance review for a sample of employees within the Information Security team to determine that performance reviews were conducted at least annually for these employees.	No exceptions noted.
		CC 1.4-09	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 1.4-10	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.	**Inquiry**: Inquired of the VP of HR to determine that personnel were required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.
				Inspection: Inspected the signed copy of the Code of Conduct for a sample of new and current employees to determine that personnel were required to read and accept the Code of Conduct, which included the statement of confidentiality and privacy practices, upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 1.4-11	The entity evaluates its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revises these when necessary to help meet changing commitments and requirements.	**Inquiry**: Inquired of the VP of Human Resources to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process and revised them when necessary to help meet changing commitments and requirements.	No exceptions noted.
				Inspection: Inspected the reporting lines in the HR system for a sample of employees to determine that the entity evaluated its organizational structure, reporting lines, authorities, and responsibilities as part of its business planning process and as part of its ongoing risk assessment and management process.	No exceptions noted.
				Inspection: Inspected an email announcement from management about the realignment of organizational personnel under new leadership to determine that the entity evaluated its organizational structure, reporting lines, authorities, as changes occurred in the organization.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	CC 1.5-01	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 1.5-02	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 1: Common Criteria Related to Control Environment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				information security policies.	
		CC 1.5-03	Performance reviews are conducted at least annually for employees within the Information Security team.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that performance reviews were conducted at least annually for employees within the Information Security team.	No exceptions noted.
				Inspection: Inspected the most recent annual performance review for a sample of employees within the Information Security team to determine that performance reviews were conducted at least annually for these employees.	No exceptions noted.
		CC 1.5-04	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	CC 2.1-01	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 2.1-02	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 2.1-03	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 2.1-04	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 2.1-05	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 2.1-06	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 2.1-07	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 2.1-08	Members of the Incident Response Team complete annual training to ensure awareness of proper escalation paths and criteria.	**Inquiry**: Inquired of the Senior Director of Information Security and Senior Software Architect to determine that members of the Incident Response Team completed annual training to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
				Inspection: Inspected evidence of completion of Incident Response training for a sample of Incident Response Team members to determine that they completed the training annually to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	CC 2.2-01	Workiva has reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, all of which are communicated to internal users in the Wlife policy repository and to external users through Workiva's public-facing website.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, which were communicated to internal users in the Wlife policy repository and to external users through Workiva's public-facing website.	No exceptions noted.
				Inspection: Inspected the Ethics Hotline information on Wlife and the third-party reporting portal on the public-facing website to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, which were communicated to internal users in the Wlife policy repository and to external users through Workiva's public-facing website.	No exceptions noted.
				Inspection: Inspected the agreement with the third-party hotline service to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				incidents and compliance concerns.	
		CC 2.2-02	The Wdesk Success Center public website is used to communicate system changes to external users and the weekly Customer Success Playbook e-mail is used to communicate system changes to internal users.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that the Wdesk Success Center public website was used to communicate system changes to external users and that the weekly Customer Success Playbook e-mail was used to communicate system changes to internal users.	No exceptions noted.
				Observation: Observed the resources available on Wdesk Success Center to determine that it was a public website and that it was used to communicate system changes to external users.	No exceptions noted.
				Inspection: Inspected e-mail evidence for a sample of weekly notifications sent to Customer Service Managers to determine that the weekly Customer Success Playbook e-mail was used to communicate system changes to internal users.	No exceptions noted.
		CC 2.2-03	System architecture diagrams depicting details (operating systems, applications, open ports and protocols) of production systems and the system boundary are maintained for use in describing and	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that system architecture diagrams depicting details of production systems and the system boundary were maintained for use in describing and auditing	No exception noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			auditing the Workiva platform environment.	the Workiva platform environment.	
				Inspection: Inspected the system architecture diagrams to determine that they were documented, maintained and provided details of production systems and the system boundary for use in describing and auditing the Workiva platform environment.	No exception noted.
		CC 2.2-04	System changes that can impact the security of the system have security reviews performed and signed off by management prior to release into production.	**Inquiry**: Inquired of the Senior Software Architect to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
				Inspection: Inspected the Development Security Guidelines to determine that they documented the process around the security reviews performed for system changes impacting the security of the system.	No exceptions noted.
				Inspection: Inspected the evidence of security review and sign off for a sample of changes to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 2.2-05	Release Management verifies Development and Quality Assurance requirements have been met prior to release into production.	**Inquiry**: Inquired of the Senior Software Architect to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
				Observation: Observed the automated process to release changes to production to determine that release management verified development and quality assurance requirements were met prior to releasing the change into production and halted the release when certain requirements were not met.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
		CC 2.2-06	A link from the Workiva platform login page makes terms of use and privacy statement available to system users, including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that a link from the Workiva platform login page made terms of use and privacy statement available to system users including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva and the	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			and the Workiva platform end user.	Workiva platform end user.	
				Inspection: Inspected the terms of use and privacy statement on the Workiva platform's login page to determine that a link from the Workiva platform login page made terms of use and privacy statement available to system users including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva and the Workiva platform end user.	No exceptions noted.
		CC 2.2-07	A help line is made available to all customers for issues, including those related to security, that need to be addressed immediately.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that a help line was made available to customers for issues, including those related to security, that need to be addressed immediately.	No exceptions noted.
				Observation: Observed the Senior IT Risk & Compliance Analyst place a call to the helpline to determine that a help line was available to customers for issues, including those related to security, that needed to be addressed immediately.	No exceptions noted.
				Inspection: Inspected the emergency contact line to determine that a help line is made available to all customers for issues, including those related to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				security, that need to be addressed immediately.	
		CC 2.2-08	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
				Inspection: Inspected the written job description and the HR job offer workflow for a sample of job positions to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
		CC 2.2-09	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and and if required, updates were made.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 2.2-10	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 2.2-11	Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm	**Inquiry**: Inquired of the VP of HR to determine that personnel were required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and formally re-	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			them annually thereafter.	affirmed them annually thereafter.	
				Inspection: Inspected the signed copy of the Code of Conduct for a sample of new and current employees to determine that personnel were required to read and accept the Code of Conduct, which included the statement of confidentiality and privacy practices, upon their hire and formally re-affirmed them annually thereafter.	No exceptions noted.
		CC 2.2-12	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry**: Inquired of the VP of HR to determine that employees were trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	No exceptions noted
				Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the	CC 2.3-01	Enforcement of Workiva's Information Security policy is the responsibility of a Chief Compliance Officer or delegate.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
	functioning of internal control.			Compliance Officer or delegate.	
				Inspection: Inspected the Information Security Policy to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
		CC 2.3-02	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry:** Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 2.3-03	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry:** Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
		CC 2.3-04	Workiva has reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, all of which are communicated to internal users in the Wlife policy repository and to external users through Workiva's public-facing website.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, which were communicated to internal users in the Wlife policy repository and to external users through Workiva's public-facing website.	No exceptions noted.
				Inspection: Inspected the Ethics Hotline information on Wlife and the third-party reporting portal on the public-facing website to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns through Workiva's public website, e-mail, or a third-party reporting hotline, which were communicated to internal users in the	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Wlife policy repository and to external users through Workiva's public-facing website.	
				Inspection: Inspected the agreement with the third-party hotline service to determine that Workiva had reporting mechanisms in place for reporting security and confidentiality incidents and compliance concerns.	No exceptions noted.
		CC 2.3-05	The Wdesk Success Center public website is used to communicate system changes to external users and the weekly Customer Success Playbook e-mail is used to communicate system changes to internal users.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that the Wdesk Success Center public website was used to communicate system changes to external users and that the weekly Customer Success Playbook e-mail was used to communicate system changes to internal users.	No exceptions noted.
				Observation: Observed the resources available on Wdesk Success Center to determine that it was a public website and that it was used to communicate system changes to external users.	No exceptions noted.
				Inspection: Inspected e-mail evidence for a sample of weekly notifications sent to Customer Service Managers to determine that the weekly Customer Success Playbook e-mail was used to communicate system changes to internal users.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 2.3-06	A link from the Workiva platform login page makes terms of use and privacy statement available to system users, including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva and the Workiva platform end user.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that a link from the Workiva platform login page made terms of use and privacy statement available to system users including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva and the Workiva platform end user.	No exceptions noted.
				Inspection: Inspected the terms of use and privacy statement on the Workiva platform's login page to determine that a link from the Workiva platform login page made terms of use and privacy statement available to system users including a definition of the system and its boundaries, and the delineation of responsibilities for security and confidentiality between Workiva and the Workiva platform end user.	No exceptions noted.
		CC 2.3-07	A help line is made available to all customers for issues, including those related to security, that need to be addressed immediately.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that a help line was made available to customers for issues, including those related to security, that need to be addressed immediately.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 2: Common Criteria Related to Communication and Information					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Observation: Observed the Senior IT Risk & Compliance Analyst place a call to the helpline to determine that a help line was available to customers for issues, including those related to security, that needed to be addressed immediately.	No exceptions noted.
				Inspection: Inspected the emergency contact line to determine that a help line is made available to all customers for issues, including those related to security, that need to be addressed immediately.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	CC 3.1-01	Roles and responsibilities are defined in written job descriptions and communicated to employees and their supervisors.	**Inquiry**: Inquired of the VP of HR to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
				Inspection: Inspected the written job description for a sample of job positions and the HR job offer workflow to determine that roles and responsibilities were defined in written job descriptions and communicated to employees and their supervisors.	No exceptions noted.
		CC 3.1-02	Job descriptions are reviewed by managers on an annual basis for needed changes and where job duty changes are required; necessary changes to these job descriptions are also made.	**Inquiry**: Inquired of the VP of HR to determine that job descriptions were reviewed by managers on an annual basis for needed changes and where job duty changes were required, necessary changes to these job descriptions were also made.	No exceptions noted.
				Inspection: Inspected the job description reviews for a sample of job descriptions to determine that job descriptions were reviewed by managers on an annual basis and and if required, updates were made.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.1-03	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 3.1-04	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.
		CC 3.1-05	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 3.1-06	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 3.1-07	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 3.1-08	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				information security policies.	
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
CC 3.2	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.	CC 3.2-01	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 3.2-02	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 3.2-03	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 3.2-04	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				confidentiality requirements.	
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
		CC 3.2-05	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry:** Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.2-06	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
		CC 3.2-07	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	
		CC 3.2-08	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 3.2-09	Third party penetration and vulnerability testing is performed semi-annually and issues identified are	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			documented and addressed.	**Inspection**: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 3.2-10	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				was triggered by automatically opening a ticket.	
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
		CC 3.2-11	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
		CC 3.2-12	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				monthly, to review and address security issues.	
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	CC 3.3-01	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 3.3-02	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.3-03	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 3.3-04	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				confidentiality requirements.	
		CC 3.3-05	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 3.3-06	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				compliance with information security policies.	
		CC 3.3-07	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 3.3-08	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 3.3-09	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				determine that issues identified were documented and addressed.	
		CC 3.3-10	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.3-11	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 3.3-12	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.3-13	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 3.3-14	Members of the Incident Response Team complete annual training to ensure awareness of proper escalation paths and criteria.	**Inquiry**: Inquired of the Senior Director of Information Security and Senior Software Architect to determine that members of the Incident Response Team completed annual training to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
				Inspection: Inspected evidence of completion of Incident Response training for a sample of Incident Response Team members to determine that they completed the training annually to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	CC 3.4-01	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 3.4-02	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				support of the production environment.	
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 3.4-03	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 3.4-04	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 3.4-05	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
		CC 3.4-06	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 3.4-07	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 3.4-08	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 3.4-09	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
		CC 3.4-10	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 3: Common Criteria Related to Risk Assessment					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 3.4-11	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 4.1	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.	CC 4.1-01	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 4.1-02	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 4.1-03	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry**: Inquired of the VP of HR to determine that employees were trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	No exceptions noted
				Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
		CC 4.1-04	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 4.1-05	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
		CC 4.1-06	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	
		CC 4.1-07	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 4.1-08	Third party penetration and vulnerability testing is performed semi-annually and issues identified are	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			documented and addressed.	**Inspection**: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 4.1-09	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				personnel when an alarm was triggered by automatically opening a ticket.	
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
CC 4.2	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.	CC 4.2-01	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment,	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				coordination among organizational entities, and compliance.	
		CC 4.2-02	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 4.2-03	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 4.2-04	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 4.2-05	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				information security policies.	
		CC 4.2-06	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 4.2-07	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 4.2-08	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 4.2-09	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 4: Common Criteria Related to Monitoring Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 4.2-10	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
		CC 4.2-11	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 5.1	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.	CC 5.1-01	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 5.1-02	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.
		CC 5.1-03	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 5.1-04	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification.	No exceptions noted.
		CC 5.1-05	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 5.1-06	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
		CC 5.1-07	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry:** Inquired of the VP of HR to determine that employees were trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	No exceptions noted
				Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
		CC 5.1-08	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry:** Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 5.1-09	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
		CC 5.1-10	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 5.1-11	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 5.1-12	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 5.1-13	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is	**Inquiry:** Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	an alarm was triggered, and that alerts were logged, tracked, and resolved.	
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
		CC 5.1-14	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification,	No exception noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				documentation, resolution, communications and escalation of computer security incidences.	
		CC 5.1-15	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
		CC 5.1-16	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.1-17	Members of the Incident Response Team complete annual training to ensure awareness of proper escalation paths and criteria.	**Inquiry**: Inquired of the Senior Director of Information Security and Senior Software Architect to determine that members of the Incident Response Team completed annual training to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
				Inspection: Inspected evidence of completion of Incident Response training for a sample of Incident Response Team members to determine that they completed the training annually to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
		CC 5.1-18	The Information Security team distributes security-related education and awareness communications to employees on a quarterly basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.
				Inspection: Inspected the Information Security communication for a sample of quarters to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.1-19	The organization maintains and publishes a Restricted Trade List and a policy is in place to prohibit employees from engaging in insider trading. An intent-to-trade process exists to allow employees to request permission to conduct trading activities.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
				Inspection: Inspected the Restricted Trade List/No Trade List to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
				Inspection: Inspected the script used to automatically update the Restricted Trade List to determine that the organization had a process to scan for and identify new accounts to add to the Restricted Trade List based on newly onboarded clients.	No exceptions noted.
				Inspection: Inspected the Insider Trading Policy to determine that a policy was in place to prohibit employees from engaging in insider trading and defined a process to allow employees to request permission to conduct trading activities.	No exceptions noted.
		CC 5.1-20	Employees with access to system administration and diagnostic tools for production systems complete annual training specific to the risks and obligations of their access.	**Inquiry**: Inquired of Senior Director of Information Security to determine that employees with access to system administration and diagnostic tools for production systems completed annual training specific to the risks and obligations of their access.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the training completion results for a sample of employees with access to system administration and diagnostic tools to determine that they completed annual training specific to the risks and obligations of their access.	No exceptions noted.
				Inspection: Inspected the Being a Wdesk Administrator training to determine that its content included information specific to the risks and obligations of the employees with access to system administration and diagnostic tools for production systems.	No exceptions noted.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	CC 5.2-01	Users are required to utilize unique User IDs to access system resources.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that users were required to utilize unique User IDs to access system resources.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security attempt to create a duplicate user ID within the single sign on tool, Okta, and not be permitted to complete the set-up to determine that users were required to utilize unique user IDs to access system resources.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the user access listings for the network and production systems to determine that users were required to utilize User IDs to access system resources, and that there were no duplicate user IDs.	No exceptions noted.
		CC 5.2-02	Employees are prohibited from sharing login credentials or using generic accounts to access production systems.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that employees were prohibited from sharing login credentials or using generic accounts to access production systems.	No exceptions noted.
				Inspection: Inspected the Identity & Access Management Policy to determine that employees were prohibited from sharing login credentials or using generic accounts to access production systems.	No exceptions noted.
		CC 5.2-03	Password requirements for in-scope systems adhere to the documented Password Policy.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that password requirements for in-scope systems adhered to the documented Password Policy.	No exceptions noted.
				Inspection: Inspected the Password Policy within the Identity and Access Management Policy to determine that password requirements	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				were defined for in-scope systems.	
				Inspection: Inspected the password settings for each in-scope system to determine that password requirements for in-scope systems adhered to the documented Password Policy.	No exceptions noted.
		CC 5.2-04	Logical access to system information, including Restricted Information, requires the use of two-factor authentication.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that logical access to system information, including restricted information, required the use of two-factor authentication.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security login to the Workiva production systems to determine that two-factor authentication was used and was required to access system information, including restricted information.	No exceptions noted.
				Inspection: Inspected the two-factor authentication configuration to determine that logical access to system information, including restricted information, required the use of two-factor authentication.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.2-05	Access to system administration functions for in-scope applications and related databases and diagnostic tools for production systems is restricted to appropriate individuals based on job function.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that access to system administration for in-scope applications and related databases, and diagnostic tools for production systems was restricted to appropriate individuals based on job function.	No exceptions noted.
				Inspection: Inspected the list of administrators for the in-scope systems and their job responsibilities to determine that access to system administration for in-scope applications and related databases, and diagnostic tools for production systems was restricted to appropriate individuals based on job function.	No exceptions noted.
		CC 5.2-06	Administrative access to Workiva's cloud networks and network protection utilities is restricted to appropriate individuals based on job function.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that administrative access to Workiva's cloud networks and network protection utilities was restricted to appropriate personnel.	No exceptions noted.
				Inspection: Inspected the list of users with administrative access to Workiva's cloud networks and utilities and their job responsibilities to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.2-07	Default user access is granted based on job responsibilities by department and approved by business unit management.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of HR to determine that default user access was granted based on job responsibilities by department and approved by business unit management.	No exceptions noted.
				Inspection: Inspected the HR profile for a sample of new hires to determine appropriate business unit management gave approval prior to hire and default access being granted.	No exceptions noted.
		CC 5.2-08	Access to systems containing Restricted-level customer information must require users to authenticate via a single sign-on system.	**Inquiry**: Inquired of the VP of IT and Senior Director of Information Security to determine that access to systems containing restricted-level customer information must require users to authenticate via a single sign-on system.	No exceptions noted.
				Observation: Observed the VP of IT authenticate into the Workiva platform containing restricted-level customer information to determine that authentication via single sign-on was required.	No exceptions noted.
				Inspection: Inspected the log-in process of the Workiva platform to determine that access required users to authenticate via a single sign-on system.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.2-09	Requests for access to production systems are authorized by the employee's manager and system owner prior to being processed.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of new access requests to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.
		CC 5.2-10	User access to Workiva's cloud networks and in-scope applications and databases is revoked within 2 business days of an employee's termination date.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
				Inspection: Inspected the ticket for a sample terminated employees and contractors and the access list to in-scope systems to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.2-11	Customer user account management requests must be appropriately authorized per customer agreement.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that customer user account management requests must be appropriately authorized per customer agreement.	No exceptions noted.
				Inspection: Inspected the Customer Data Access Policy to determine that customer user account management requests were required to be appropriately authorized per customer agreement.	No exceptions noted.
				Inspection: Inspected the client request for a sample of new customer access granted to determine that customer user account management requests were appropriately authorized per customer agreement.	No exceptions noted.
		CC 5.2-12	User access is reviewed and certified by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that user access was reviewed and certified by management on a semi-annual basis.	No exceptions noted
				Inspection: Inspected the most recent user access review for the in-scope systems to determine that user access reviews were performed and certified by management semi-annually.	No exceptions noted

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.2-13	System Development Life Cycle policies and procedures are in place.	**Inquiry**: Inquired of the Senior Software Architect to determine that System Development Life Cycle policies and procedures were in place.	No exceptions noted.
				Inspection: Inspected the Application Security Standard to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
				Inspection: Inspected the Development Security Review procedure and the SDLC process flow chart to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
		CC 5.2-14	Quality assurance testing procedures are performed and documented for code changes to the production environment.	**Inquiry**: Inquired of the Senior Software Architect to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
		CC 5.2-15	Separate Test, Development, and Production environments are	**Inquiry**: Inquired of the Senior Software Architect to determine that separate test, development, and production environments	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			maintained for the Workiva platform.	were maintained for the Workiva platform.	
				Observation: Observed the test, development and production environments for the Workiva platform to determine that separate environments were maintained.	No exceptions noted.
		CC 5.2-16	Segregation of responsibilities for code changes to the production environment is maintained between development, code review, and release processes.	**Inquiry**: Inquired of the Senior Software Architect to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
				Inspection: Inspected the System Development Life Cycle process flow chart to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases showing the individuals who performed code review and QA review and the automated release tool that pushed the release to production to determine that separate individuals performed code review, QA review, and release signoff showing segregation of responsibilities for code changes to the production	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				environment was maintained between development, code review, and release processes.	
		CC 5.2-17	Customer data is restricted to only authorized users.	**Inquiry**: Inquired of the Director, Global Services Operations to determine that customer data was restricted to only authorized users.	No exceptions noted.
				Observation: Observed the Senior Operations Coordinator provision access to customer data to determine that customer data was restricted through the use of administrator groups.	No exceptions noted.
				Inspection: Inspected users with Super Administrator privileges and System Administrator privileges and their job responsibilities to determine that they were aligned with departments approved by management to have customer data access, and confirmed that customer data was restricted to authorized users based on their job function.	No exceptions noted.
		CC 5.2-18	Workiva policy requires confidential data to be de-identified prior to use in testing or movement into other non-production environments.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva policy required confidential data to be de-identified prior to use in testing or movement into other non-production environments.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Observation: Observed the Senior Director of Information Security access data within the test environment to determine that the data was sanitized, and confirmed that Workiva de-identified data according to policy prior to use in testing or movement into other non-production environments.	No exceptions noted.
				Inspection: Inspected the Application Development Policy to determine that Workiva policy required confidential data to be de-identified prior to use in testing or movement into other non-production environments.	No exceptions noted.
		CC 5.2-19	Customer Success leadership (Workiva platform Super Administrators) complete annual training specific to the risks and obligations of their role in administering accounts and users.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Customer Success leadership (Workiva platform Super Administrators) completed annual training specific to the risks and obligations of their role in administering accounts and users.	No exceptions noted.
				Inspection: Inspected the certificate of completion for the Being a Wdesk Super Admin training for a sample of super administrators to determine that Customer Success leadership completed annual training specific to the risks and obligations of their role in	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				administering accounts and users.	
				Inspection: Inspected the super admin training material to determine that the training content included information relevant to risks and obligations of the Customer Success leadership's role in administering accounts and users.	No exceptions noted.
		CC 5.2-20	Policy requires personnel issued Workiva devices to use only such devices when handling restricted data.	**Inquiry:** Inquired of the Senior Director of Information Security to determine policy required personnel issued Workiva devices to use only such devices when handling restricted data.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that it required personnel issued Workiva devices to use only such devices when handling restricted data.	No exceptions noted.
		CC 5.2-21	System changes that can impact the security of the system have security reviews performed and signed off by management prior to release into production.	**Inquiry**: Inquired of the Senior Software Architect to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
				Inspection: Inspected the Development Security Guidelines to determine that they documented the process around the security reviews performed for system changes	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				impacting the security of the system.	
				Inspection: Inspected the evidence of security review and sign off for a sample of changes to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
		CC 5.2-22	Release Management verifies Development and Quality Assurance requirements have been met prior to release into production.	**Inquiry**: Inquired of the Senior Software Architect to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
				Observation: Observed the automated process to release changes to production to determine that release management verified development and quality assurance requirements were met prior to releasing the change into production and halted the release when certain requirements were not met.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	CC 5.3-01	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
		CC 5.3-02	Entity policies include suspension of access, up to and including termination, as potential sanctions for employee misconduct.	**Inquiry**: Inquired of the VP of HR to determine that entity policies included suspension of access, up to and including termination, as potential sanctions for employee misconduct.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Code of Conduct and the Personnel Security Policy to determine that entity policies included suspension of access, up to and including termination as potential sanctions for employee misconduct.	No exceptions noted.
		CC 5.3-03	Enforcement of Workiva's Information Security policy is the responsibility of a Chief Compliance Officer or delegate.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that enforcement of Workiva's Information Security Policy was the responsibility of a Chief Compliance Officer or delegate.	No exceptions noted.
		CC 5.3-04	Documentation of internal processes, policies and procedures is available on the Workiva intranet and retained for at least 6 years.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that processes, policies and procedures were documented and published on the Company intranet.	No exceptions noted.
				Inspection: Inspected the storage location of processes, policies and procedures to determine that they were available on the Company intranet.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.3-05	Employees are trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	**Inquiry**: Inquired of the VP of HR to determine that employees were trained on Security Awareness and the Customer Confidentiality and Securities Trading Policy upon hire and annually.	No exceptions noted
				Inspection: Inspected the training completion results of the Security Awareness and the Information Security & Securities Trading policy for a sample of new hires, existing employees, and contractors to determine the trainings were completed upon hire and annually.	No exceptions noted
		CC 5.3-06	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 5.3-07	The Information Security team distributes security-related education and awareness communications to employees on a quarterly basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.
				Inspection: Inspected the Information Security communication for a sample of quarters to determine that the Information Security team distributed security-related education and awareness communications to employees on a quarterly basis.	No exceptions noted.
		CC 5.3-08	The organization maintains and publishes a Restricted Trade List and a policy is in place to prohibit employees from engaging in insider trading. An intent-to-trade process exists to allow employees to request permission to conduct trading activities.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
				Inspection: Inspected the Restricted Trade List/No Trade List to determine that the organization maintained and published a Restricted Trade List.	No exceptions noted.
				Inspection: Inspected the script used to automatically update the Restricted Trade List to determine that the organization had a process to scan for and identify new accounts to add to the Restricted Trade List	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 5: Common Criteria Related to Control Activities					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				based on newly onboarded clients.	
				Inspection: Inspected the Insider Trading Policy to determine that a policy was in place to prohibit employees from engaging in insider trading and defined a process to allow employees to request permission to conduct trading activities.	No exceptions noted.
		CC 5.3-09	Employees with access to system administration and diagnostic tools for production systems complete annual training specific to the risks and obligations of their access.	**Inquiry**: Inquired of Senior Director of Information Security to determine that employees with access to system administration and diagnostic tools for production systems completed annual training specific to the risks and obligations of their access.	No exceptions noted.
				Inspection: Inspected the training completion results for a sample of employees with access to system administration and diagnostic tools to determine that they completed annual training specific to the risks and obligations of their access.	No exceptions noted.
				Inspection: Inspected the Being a Wdesk Administrator training to determine that its content included information specific to the risks and obligations of the employees with access to system administration and diagnostic tools for production systems.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 6.1	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.	CC 6.1-01	Access to the backup tool is restricted to members of the infrastructure team.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that access to the backup tool was restricted to members of the infrastructure team.	No exceptions noted.
				Inspection: Inspected the listing of users with access to the backup tool and their job responsibilities to determine that access was restricted to members of the Infrastructure team.	No exceptions noted.
		CC 6.1-02	Backup files are encrypted using Advanced Encryption Standards.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that backups files were encrypted using Advanced Encryption Standards.	No exceptions noted.
				Inspection: Inspected the configuration of backup settings within Google Cloud and the encryption used for AWS to determine that backup files were encrypted using Advanced Encryption Standards.	No exceptions noted.
		CC 6.1-03	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.
		CC 6.1-04	Communication sessions between the Workiva product and user organizations are secured using TLS encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.
				Inspection: Inspected the digital certificate and encryption configuration for the Workiva product to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.
		CC 6.1-05	Workiva policy defines, and employee training reinforces, acceptable channels through which restricted-level customer data can be transferred in accordance with security and confidentiality obligations.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that Workiva policy defined, and employee training reinforced, acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Information Security Policy to determine that Workiva policy defined acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
				Inspection: Inspected the IT security training to determine that it reinforced acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
		CC 6.1-06	Customer data is encrypted at rest using AES256 encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that customer data was encrypted at rest using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected the encryption configuration for the Google Cloud Platform managed by Workiva and the native encryption method used and managed by Amazon Web Services to determine customer data was encrypted using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected a sample client's data within Google Cloud to determine that customer data was encrypted using AES-256 encryption.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.1-07	Configuration hardening guidelines are documented to define the configuration of production systems.	**Inquiry**: Inquired of the Senior Software Architect to determine that configuration hardening guidelines were documented to define the configuration of production systems.	No exceptions noted.
				Observation: Observed the script file used to configure production systems on a sample system to determine that configuration hardening guidelines were defined for the configuration of production systems.	No exceptions noted.
				Inspection: Inspected the configuration hardening guidelines to determine that such guidelines were documented to define the configuration of production systems.	No exceptions noted.
		CC 6.1-08	Production systems are kept in conformance to hardening guidelines through the use of continuous compliance scanning.	**Inquiry**: Inquired of the Senior Software Architect to determine that production systems were kept in conformance to hardening guidelines through the use of continuous compliance scanning.	No exceptions noted.
				Observation: Observed the configuration of the entity's production host monitoring tool to determine that it scanned production systems to verify they were in conformance to hardening guidelines, and generated an alert when systems were identified as being in	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				compliance with guidelines.	
				Inspection: Inspected the log of alerts resulting from the continuous compliance scanning along with the resolution status to determine that production systems were scanned for conformance with hardening guidelines, and that alerts were auto-generated by the tool when changes were made that led to non-conformance and addressed.	No exceptions noted.
		CC 6.1-09	The default inactivity timeout configuration in the Workiva platform is 60 minutes by default, and can be customized by the customer account administrator.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that the default inactivity timeout configuration in the Workiva platform was 60 minutes by default, which could be customized by the customer account administrator.	No exception noted.
				Inspection: Inspected the configuration for Wdesk timeout setting to determine that the default inactivity timeout configuration in the Workiva platform was 60 minutes by default, which could be customized by the customer account administrator.	No exception noted.
		CC 6.1-10	Internet-facing production systems are configured to restrict incoming traffic to approved locations.	**Inquiry**: Inquired of the Senior Software Architect to determine that internet-facing production systems were configured to restrict incoming traffic to approved locations.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Amazon Web Service security group configuration for internet-facing production systems to determine that traffic restrictions were configured to restrict incoming traffic to approved locations.	No exceptions noted.
		CC 6.1-11	The IT department conducts an annual review of all unassigned Workiva-owned laptops to determine whether unassigned laptops are in use. Workiva policy prohibits assets without an owner assigned from use.	**Inquiry**: Inquired of the Senior IT Support Specialist to determine that the IT department conducted an annual review of unassigned Workiva-owned laptops to determine whether unassigned laptops were in use.	No exceptions noted.
				Inspection: Inspected the most recent review of unassigned Workiva-owned laptops to determine that the IT department conducted an annual review of unassigned Workiva-owned laptops to verify whether they were in use.	No exceptions noted.
				Inspection: Inspected the Information Asset Management Policy to determine that Workiva policy prohibited assets without an owner assigned from use.	No exceptions noted.
		CC 6.1-12	System administration tasks require the use of a multi-factor authenticated bastion to access consoles.	**Inquiry**: Inquired of the Senior Software Architect to determine that system administration tasks required the use of a multi-factor authenticated Bastion to access consoles.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Observation: Observed the Senior Software Architect access a production console through the use of a multi-factor authenticated bastion, which required the user to verify the access attempt both using their online account and on their mobile device, to determine that system administration tasks required the use of multi-factor authentication bastion to access consoles.	No exceptions noted.
		CC 6.1-13	Software is used to log user activities in Workiva production hosts and the InfoSec team reviews the logs to identify and address unauthorized access to or modification of Workiva production databases.	**Inquiry**: Inquired of the Senior Software Architect to determine that software was used to monitor and alert for unauthorized access to or modification of Workiva production databases, and that alerts were reviewed and addressed.	No exceptions noted.
				Observation: Observed the configuration of the script in the monitoring software to determine that software was used to log user activities in Workiva production databases.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of user activity generated alerts to determine that the InfoSec team reviewed the log of activities to identify and address unauthorized access to or modification of Workiva production databases.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.1-14	Direct access to production databases is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that direct access to production databases was restricted to appropriate personnel based on job function.	No exceptions noted.
				Inspection: Inspected the list of users with direct access to production databases and their job responsibilities to determine that direct access to production databases was restricted to appropriate personnel based on job function.	No exceptions noted.
		CC 6.1-15	Workiva maintains a role to access mapping for the Workiva platform administrative, Google Cloud Platform, and Amazon Web Services environments.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva maintained a role to access mapping for the Workiva platform administrative, Google Cloud Platform, and Amazon Web Services environments.	No exceptions noted.
				Inspection: Inspected the role to access mapping document to determine the Workiva maintained a role to access mapping, which documented the alignment between roles and access to security functions for the Workiva platform administrative, Google Cloud Platform, and Amazon Web Services environments.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.1-16	The ability to modify data transmission protocols controlling the flow of information between systems within the production environment is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that the ability to modify data transmission protocols controlling the flow of information between systems within the production environment was restricted to appropriate personnel.	No exceptions noted.
				Inspection: Inspected the listing of users with the ability to modify data transmission protocols and their job responsibilities to determine that the users' access was appropriate based on their job function.	No exceptions noted.
		CC 6.1-17	Devices of users with access to Restricted level data are encrypted in accordance with the requirements of the Encryption Standard.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that devices of users with access to Restricted-level data were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
				Inspection: Inspected the encryption settings for a sample of user devices with access to Restricted-level data to determine that the devices were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
		CC 6.1-18	Removable media (e.g. thumb drives) is restricted to read-only for users with	**Inquiry**: Inquired of the SaaS Operations Engineer to determine that removable media was restricted to read-only for	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			access to Restricted information.	users with access to restricted information.	
				Inspection: Inspected the configuration settings for the endpoint protection software to determine that removable storage devices were blocked and restricted to read-only.	No exceptions noted.
		CC 6.1-19	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
		CC 6.1-20	Customer SEC filing activities are logged and monitored with automated alerts.	**Inquiry:** Inquired of the Senior Software Architect to determine that customer SEC filing activities were logged and monitored with automated alerts.	No exceptions noted.
				Inspection: Inspected the list of Customer SEC filings and the automated alert for a sample of Customer SEC filings to determine that customer SEC filing activities were logged and monitored with automated alerts	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.1-21	Access to system administration functions for in-scope applications and related databases and diagnostic tools for production systems is restricted to appropriate individuals based on job function.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that access to system administration for in-scope applications and related databases, and diagnostic tools for production systems was restricted to appropriate individuals based on job function.	No exceptions noted.
				Inspection: Inspected the list of administrators for the in-scope systems and their job responsibilities to determine that access to system administration for in-scope applications and related databases, and diagnostic tools for production systems was restricted to appropriate individuals based on job function.	No exceptions noted.
		CC 6.1-22	Administrative access to Workiva's cloud networks and network protection utilities is restricted to appropriate individuals based on job function.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that administrative access to Workiva's cloud networks and network protection utilities was restricted to appropriate personnel.	No exceptions noted.
				Inspection: Inspected the list of users with administrative access to Workiva's cloud networks and utilities and their job responsibilities to determine that access was restricted to appropriate individuals based on job function.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.1-23	User access to Workiva's cloud networks and in-scope applications and databases is revoked within 2 business days of an employee's termination date.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
				Inspection: Inspected the ticket for a sample terminated employees and contractors and the access list to in-scope systems to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
CC 6.2	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.	CC 6.2-01	Default user access is granted based on job responsibilities by department and approved by business unit management.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of HR to determine that default user access was granted based on job responsibilities by department and approved by business unit management.	No exceptions noted.
				Inspection: Inspected the HR profile for a sample of new hires to determine appropriate business unit management gave approval prior to hire and default access being granted.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.2-02	Requests for access to production systems are authorized by the employee's manager and system owner prior to being processed.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of new access requests to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.
		CC 6.2-03	User access to Workiva's cloud networks and in-scope applications and databases is revoked within 2 business days of an employee's termination date.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
				Inspection: Inspected the ticket for a sample terminated employees and contractors and the access list to in-scope systems to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.2-04	Customer user account management requests must be appropriately authorized per customer agreement.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that customer user account management requests must be appropriately authorized per customer agreement.	No exceptions noted.
				Inspection: Inspected the Customer Data Access Policy to determine that customer user account management requests were required to be appropriately authorized per customer agreement.	No exceptions noted.
				Inspection: Inspected the client request for a sample of new customer access granted to determine that customer user account management requests were appropriately authorized per customer agreement.	No exceptions noted.
		CC 6.2-05	User access is reviewed and certified by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that user access was reviewed and certified by management on a semi-annual basis.	No exceptions noted
				Inspection: Inspected the most recent user access review for the in-scope systems to determine that user access reviews were performed and certified by management semi-annually.	No exceptions noted
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and	CC 6.3-01	The Workiva Onboarding system automatically provisions access to in-scope systems based on employee	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of IT to determine that the Workiva onboarding system	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
	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.		role for new hires, where supported.	automatically provisioned access to the in-scope systems based on employee role for new hires, where supported.	
				Inspection: Inspected the defined departmental standard access profile and the ticket logging the access granted for a sample of new hires to determine that access was automatically granted to the in-scope system based on employee role.	No exceptions noted.
		CC 6.3-02	Default user access is granted based on job responsibilities by department and approved by business unit management.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of HR to determine that default user access was granted based on job responsibilities by department and approved by business unit management.	No exceptions noted.
				Inspection: Inspected the HR profile for a sample of new hires to determine appropriate business unit management gave approval prior to hire and default access being granted.	No exceptions noted.
		CC 6.3-03	Requests for access to production systems are authorized by the employee's manager and system owner prior to being processed.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the ticket for a sample of new access requests to determine that requests for access to production systems were authorized by the employee's manager and system owner prior to being processed.	No exceptions noted.
		CC 6.3-04	User access to Workiva's cloud networks and in-scope applications and databases is revoked within 2 business days of an employee's termination date.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
				Inspection: Inspected the ticket for a sample terminated employees and contractors and the access list to in-scope systems to determine that user access to Workiva's cloud networks and in-scope applications and databases was revoked within 2 business days of an employee's termination date.	No exceptions noted.
		CC 6.3-05	Customer user account management requests must be appropriately authorized per customer agreement.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that customer user account management requests must be appropriately authorized per customer agreement.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Customer Data Access Policy to determine that customer user account management requests were required to be appropriately authorized per customer agreement.	No exceptions noted.
				Inspection: Inspected the client request for a sample of new customer access granted to determine that customer user account management requests were appropriately authorized per customer agreement.	No exceptions noted.
		CC 6.3-06	User access is reviewed and certified by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst to determine that user access was reviewed and certified by management on a semi-annual basis.	No exceptions noted
				Inspection: Inspected the most recent user access review for the in-scope systems to determine that user access reviews were performed and certified by management semi-annually.	No exceptions noted
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media	CC 6.4-01	Access to corporate facilities is reviewed on a semi-annual basis.	**Inquiry**: Inquired of the Director of Information Technology and the Compliance Auditor to determine that access to corporate facilities was reviewed on a semi-annual basis.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
	storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			**Inspection**: Inspected the most recent review of physical access to Workiva facilities to determine that access to corporate facilities was reviewed on a semi-annual basis and actions taken to address issues noted.	No exceptions noted.
		CC 6.4-02	Exterior and telecommunication room entrances are monitored by cameras and recordings are retained for a 90 day period. (Tier I and II Sites)	**Inquiry**: Inquired of the Director of Information Technology to determine that exterior and telecommunication room entrances were monitored by cameras and recordings were retained for a 90 day period.	No exceptions noted.
				Observation: Observed the presence of cameras at the Workiva headquarters to determine that exterior and telecommunication room entrances were monitored by cameras.	No exceptions noted.
				Inspection: Inspected the camera monitoring console and the retention setting on the logs to determine that security cameras were in place to monitoring exterior and telecommunication room entrances at various Workiva locations, and that recordings were retained for a 90 day period.	No exceptions noted.
		CC 6.4-03	Badge readers control access in and out of Workiva facilities.	**Inquiry**: Inquired of the Director of Information Technology to determine that badge readers controlled access in and out of Workiva facilities.	No exceptions noted

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Observation: Observed the use of badge readers by Workiva personnel for entering and maneuvering through the Workiva headquarters to determine that badge readers controlled access in and out of Workiva facilities.	No exceptions noted
				Inspection: Inspected the Personnel Management Policy to determine that badge readers were required to control access in and out of Workiva facilities.	No exceptions noted
				Inspection: Inspected the access list from the badge system to determine that badge readers were required to control access in and out of Workiva facilities.	No exceptions noted.
		CC 6.4-04	Access to operational work areas and computer rooms are controlled and appropriately secured.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that access to operational work areas and computer rooms was controlled and appropriately secured.	No exceptions noted.
				Inspection: Inspected the access list from the badge system to determine that access to operational work areas and computer rooms was controlled and appropriately secured.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.4-05	Operational access to the badging system controlling physical access to Workiva facilities is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Director of Information Technology to determine that operational access to the badging system controlling physical access to Workiva facilities was restricted to appropriate personnel based on job function.	No exceptions noted.
				Inspection: Inspected the listing of users with access to manage the badging system and their job responsibilities to determine that the access was restricted to appropriate personnel based on job function.	No exceptions noted.
		CC 6.4-06	Visitors are required to sign in at the reception desk. (Tier I and II Sites).	**Inquiry**: Inquired of the Chief Administrative Officer to determine that visitors were required to sign-in at the reception desk.	No exceptions noted.
				Observation: Observed the visitor sign-in process at the Workiva headquarters during various visits to determine that visitors were required to sign in at the reception desk.	No exceptions noted.
				Inspection: Inspected the visitors log for various Workiva office locations to determine that visitors' access was logged and retained.	No exceptions noted.
		CC 6.4-07	Visitors accessing areas where Restricted information is handled must sign a non-disclosure	**Inquiry**: Inquired of the Chief Administration Officer to determine that visitors accessing areas where Restricted information was handled	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			agreement. (Tier I and II Sites).	must sign a non-disclosure agreement.	
				Observation: Observed the visitor sign in process to determine that visitors accessing areas where restricted information was handled had to sign a non-disclosure agreement, which was a step in the visitor sign in process.	No exceptions noted.
				Inspection: Inspected the email receipt of the non-disclosure agreement signed by visitors to determine that it was automatically sent to the visitor by the logging tool upon signing in.	No exceptions noted.
CC 6.5	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.	CC 6.5-01	A process is in place to destroy customer data when requested by the customer.	**Inquiry**: Inquired of the VP of IT and Senior Director of Information Security to determine that a process was in place to destroy customer data when requested by the customer.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of customer data destruction requests to determine that a process was in place to destroy customer data upon request.	No exceptions noted.
		CC 6.5-02	Equipment that has stored non-public information must be sanitized in accordance with the Equipment Disposal Procedure before it can be disposed of or used for other purposes (including	**Inquiry**: Inquired of the Senior Software Architect to determine that equipment that has stored non-public information was sanitized in accordance with the Equipment Disposal Procedure before it was disposed of or re-used.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
			internal and removable media).	**Observation**: Observed the process of wiping a machine after use to determine that equipment that has stored non-public information was sanitized in accordance with the Equipment Disposal Procedure before it was disposed of or re-used.	No exceptions noted.
				Inspection: Inspected the Equipment Disposal Procedure to determine that a baseline procedure was in place for sanitization of equipment that had stored non-public information.	No exceptions noted.
				Inspection: Inspected the disposal documentation for a sample of decommissioned equipment to determine that the equipment was sanitized in accordance with the Equipment Disposal Procedure prior to disposal.	No exceptions noted.
		CC 6.5-03	Paper containing confidential information is destroyed by shredding or by placing in a designated shredding receptacle. Destruction is validated through the receipt of a certificate of destruction.	**Inquiry**: Inquired of the Chief Administration Officer to determine that paper containing confidential information was destroyed by shredding or by placing in a designated shredding receptacle and that destruction was validated through the receipt of a certificate of destruction.	No exceptions noted.
				Observation: Observed the shred bins throughout the headquarters to determine that shredding receptacles were made	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				available to dispose of paper containing confidential information.	
				Inspection: Inspected the Information Asset Management Policy and the agreement with the shredding vendor to determine that a process and vendor were in place to destroy items disposed off in the shredding receptacle.	No exceptions noted.
				Inspection: Inspected the certificate of destruction for a sample of months to determine that destruction of confidential information placed in shredding receptacles was validated through the receipt of a certificate of destruction.	No exceptions noted.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	CC 6.6-01	Anti-malware programs are installed on all laptops and servers.	**Inquiry**: Inquired of the Endpoint Administrator to determine that anti-malware programs were installed on laptops and servers.	No exceptions noted.
				Observation: Observed the antivirus tool's administration console showing the devices configured with endpoint protection to determine that an anti-malware program was installed on endpoint devices.	No exceptions noted.
				Inspection: Inspected the antivirus administration console showing devices not configured with endpoint protection entity devices to determine that there were no laptops or	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				servers connected to the environment without anti-malware installed.	
		CC 6.6-02	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 6.6-03	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 6.6-04	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				identified were documented and addressed.	
		CC 6.6-05	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.6-06	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 6.6-07	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.6-08	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 6.6-09	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.
		CC 6.6-10	Communication sessions between the Workiva product and user organizations are	**Inquiry**: Inquired of the Senior Software Architect to determine that communication sessions between the Workiva product and user	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			secured using TLS encryption.	organizations were secured using TLS encryption.	
				Inspection: Inspected the digital certificate and encryption configuration for the Workiva product to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.
		CC 6.6-11	Workiva policy defines, and employee training reinforces, acceptable channels through which restricted-level customer data can be transferred in accordance with security and confidentiality obligations.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that Workiva policy defined, and employee training reinforced, acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that Workiva policy defined acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
				Inspection: Inspected the IT security training to determine that it reinforced acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.6-12	Customer data is encrypted at rest using AES256 encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that customer data was encrypted at rest using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected the encryption configuration for the Google Cloud Platform managed by Workiva and the native encryption method used and managed by Amazon Web Services to determine customer data was encrypted using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected a sample client's data within Google Cloud to determine that customer data was encrypted using AES-256 encryption.	No exceptions noted.
		CC 6.6-13	Configuration hardening guidelines are documented to define the configuration of production systems.	**Inquiry**: Inquired of the Senior Software Architect to determine that configuration hardening guidelines were documented to define the configuration of production systems.	No exceptions noted.
				Observation: Observed the script file used to configure production systems on a sample system to determine that configuration hardening guidelines were defined for the configuration of production systems.	No exceptions noted.
				Inspection: Inspected the configuration hardening guidelines to determine that such guidelines were documented to define the	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				configuration of production systems.	
		CC 6.6-14	Production systems are kept in conformance to hardening guidelines through the use of continuous compliance scanning.	**Inquiry**: Inquired of the Senior Software Architect to determine that production systems were kept in conformance to hardening guidelines through the use of continuous compliance scanning.	No exceptions noted.
				Observation: Observed the configuration of the entity's production host monitoring tool to determine that it scanned production systems to verify they were in conformance to hardening guidelines, and generated an alert when systems were identified as being in compliance with guidelines.	No exceptions noted.
				Inspection: Inspected the log of alerts resulting from the continuous compliance scanning along with the resolution status to determine that production systems were scanned for conformance with hardening guidelines, and that alerts were auto-generated by the tool when changes were made that led to non-conformance and addressed.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.6-15	The default inactivity timeout configuration in the Workiva platform is 60 minutes by default, and can be customized by the customer account administrator.	**Inquiry**: Inquired of the Director of Global Services Operations to determine that the default inactivity timeout configuration in the Workiva platform was 60 minutes by default, which could be customized by the customer account administrator.	No exception noted.
				Inspection: Inspected the configuration for Wdesk timeout setting to determine that the default inactivity timeout configuration in the Workiva platform was 60 minutes by default, which could be customized by the customer account administrator.	No exception noted.
		CC 6.6-16	Internet-facing production systems are configured to restrict incoming traffic to approved locations.	**Inquiry**: Inquired of the Senior Software Architect to determine that internet-facing production systems were configured to restrict incoming traffic to approved locations.	No exceptions noted.
				Inspection: Inspected the Amazon Web Service security group configuration for internet-facing production systems to determine that traffic restrictions were configured to restrict incoming traffic to approved locations.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.6-17	The ability to modify data transmission protocols controlling the flow of information between systems within the production environment is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that the ability to modify data transmission protocols controlling the flow of information between systems within the production environment was restricted to appropriate personnel.	No exceptions noted.
				Inspection: Inspected the listing of users with the ability to modify data transmission protocols and their job responsibilities to determine that the users' access was appropriate based on their job function.	No exceptions noted.
		CC 6.6-18	Devices of users with access to Restricted level data are encrypted in accordance with the requirements of the Encryption Standard.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that devices of users with access to Restricted-level data were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
				Inspection: Inspected the encryption settings for a sample of user devices with access to Restricted-level data to determine that the devices were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
		CC 6.6-19	Removable media (e.g. thumb drives) is restricted to read-only for users with	**Inquiry**: Inquired of the SaaS Operations Engineer to determine that removable media was restricted to read-only for	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			access to Restricted information.	users with access to restricted information.	
				Inspection: Inspected the configuration settings for the endpoint protection software to determine that removable storage devices were blocked and restricted to read-only.	No exceptions noted.
		CC 6.6-20	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
CC 6.7	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.	CC 6.7-01	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				assessments to identify vulnerabilities.	
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 6.7-02	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 6.7-03	Third party penetration and vulnerability testing	**Inquiry**: Inquired of the Senior Director of Information Security to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			is performed semi-annually and issues identified are documented and addressed.	determine that third party penetration and vulnerability testing is performed semi-annually.	
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 6.7-04	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			incident response personnel.	**Observation**: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
		CC 6.7-05	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.7-06	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
		CC 6.7-07	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 6.7-08	Backup files are encrypted using Advanced Encryption Standards.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that backups files were encrypted using Advanced Encryption Standards.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the configuration of backup settings within Google Cloud to determine backup files were encrypted using Advanced Encryption Standards.	No exceptions noted.
		CC 6.7-09	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.
		CC 6.7-10	Communication sessions between the Workiva product and user organizations are secured using TLS encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.
				Inspection: Inspected the digital certificate and encryption configuration for the Workiva product to determine that communication sessions between the Workiva product and user organizations were secured using TLS encryption.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.7-11	Workiva policy defines, and employee training reinforces, acceptable channels through which restricted-level customer data can be transferred in accordance with security and confidentiality obligations.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that Workiva policy defined, and employee training reinforced, acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
				Inspection: Inspected the Information Security Policy to determine that Workiva policy defined acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
				Inspection: Inspected the IT security training to determine that it reinforced acceptable channels through which restricted-level customer data could be transferred in accordance with security and confidentiality obligations.	No exceptions noted.
		CC 6.7-12	Customer data is encrypted at rest using AES256 encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that customer data was encrypted at rest using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected the encryption configuration for the Google Cloud Platform managed by Workiva and the native	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				encryption method used and managed by Amazon Web Services to determine customer data was encrypted using AES-256 encryption.	
				Inspection: Inspected a sample client's data within Google Cloud to determine that customer data was encrypted using AES-256 encryption.	No exceptions noted.
		CC 6.7-13	Internet-facing production systems are configured to restrict incoming traffic to approved locations.	**Inquiry**: Inquired of the Senior Software Architect to determine that internet-facing production systems were configured to restrict incoming traffic to approved locations.	No exceptions noted.
				Inspection: Inspected the Amazon Web Service security group configuration for internet-facing production systems to determine that traffic restrictions were configured to restrict incoming traffic to approved locations.	No exceptions noted.
		CC 6.7-14	The ability to modify data transmission protocols controlling the flow of information between systems within the production environment is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that the ability to modify data transmission protocols controlling the flow of information between systems within the production environment was restricted to appropriate personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the listing of users with the ability to modify data transmission protocols and their job responsibilities to determine that the users' access was appropriate based on their job function.	No exceptions noted.
		CC 6.7-15	Devices of users with access to Restricted level data are encrypted in accordance with the requirements of the Encryption Standard.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that devices of users with access to Restricted-level data were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
				Inspection: Inspected the encryption settings for a sample of user devices with access to Restricted-level data to determine that the devices were encrypted in accordance with the requirements of the Encryption Standard.	No exceptions noted.
		CC 6.7-16	Removable media (e.g. thumb drives) is restricted to read-only for users with access to Restricted information.	**Inquiry**: Inquired of the SaaS Operations Engineer to determine that removable media was restricted to read-only for users with access to restricted information.	No exceptions noted.
				Inspection: Inspected the configuration settings for the endpoint protection software to determine that removable storage devices were blocked and restricted to read-only.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.7-17	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	CC 6.8-01	Starting June 2019, static code analysis is performed monthly. Issues identified are triaged and remediated according to Workiva's documented remediation timelines.	**Inquiry**: Inquired of the Director of Information Security to determine that starting June 2019, static code analysis was performed monthly and that issues identified were triaged and remediated according to Workiva's documented remediation timelines.	No exceptions noted.
				Inspection: Inspected the results of the static code analysis performed for a sample of months since June 2019 to determine that static code analysis was performed monthly and issues identified were triaged and remediated.	No exceptions noted.
				Inspection: Inspected the results of the static code analysis performed for a sample of months since June 2019 to determine that there were no issues identified.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 6.8-02	Version control software is in place to manage current versions of source code for the in-scope applications. The ability to modify source code for the in-scope applications is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Software Architect to determine that version control software was in place to manage current versions of source code for the in-scope applications and the ability to modify source code for the in-scope applications was restricted to appropriate personnel based on job function.	No exceptions noted.
				Observation: Observed the Senior Software Architect attempt to merge a change into production without appropriate Release Management approval and the change being blocked from release to production to determine that the ability to modify source code for the in-scope application was restricted appropriately.	No exceptions noted.
				Inspection: Inspected the list of users with access to modify source code and their job responsibilities to determine that the ability was restricted to appropriate personnel based on job function.	No exceptions noted.
		CC 6.8-03	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 6.8-04	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically create a ticket for review.	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 6.8-05	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 6.8-06	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are	**Inquiry:** Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered,	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			logged, tracked, and resolved by security incident response personnel.	and that alerts were logged, tracked, and resolved.	
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.
		CC 6.8-07	Segregation of responsibilities for code changes to the production environment is maintained between development, code review, and release processes.	**Inquiry**: Inquired of the Senior Software Architect to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
				Inspection: Inspected the System Development Life Cycle process flow chart to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the ticket for a sample of releases showing the individuals who performed code review and QA review and the automated release tool that pushed the release to production to determine that separate individuals performed code review, QA review, and release signoff showing segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
		CC 6.8-08	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.
		CC 6.8-09	Configuration hardening guidelines are documented to define the configuration of production systems.	**Inquiry**: Inquired of the Senior Software Architect to determine that configuration hardening guidelines were documented to define the	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				configuration of production systems.	
				Observation: Observed the script file used to configure production systems on a sample system to determine that configuration hardening guidelines were defined for the configuration of production systems.	No exceptions noted.
				Inspection: Inspected the configuration hardening guidelines to determine that such guidelines were documented to define the configuration of production systems.	No exceptions noted.
		CC 6.8-10	Production systems are kept in conformance to hardening guidelines through the use of continuous compliance scanning.	**Inquiry**: Inquired of the Senior Software Architect to determine that production systems were kept in conformance to hardening guidelines through the use of continuous compliance scanning.	No exceptions noted.
				Observation: Observed the configuration of the entity's production host monitoring tool to determine that it scanned production systems to verify they were in conformance to hardening guidelines, and generated an alert when systems were identified as being in compliance with guidelines.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the log of alerts resulting from the continuous compliance scanning along with the resolution status to determine that production systems were scanned for conformance with hardening guidelines, and that alerts were auto-generated by the tool when changes were made that led to non-conformance and addressed.	No exceptions noted.
		CC 6.8-11	Internet-facing production systems are configured to restrict incoming traffic to approved locations.	**Inquiry**: Inquired of the Senior Software Architect to determine that internet-facing production systems were configured to restrict incoming traffic to approved locations.	No exceptions noted.
				Inspection: Inspected the Amazon Web Service security group configuration for internet-facing production systems to determine that traffic restrictions were configured to restrict incoming traffic to approved locations.	No exceptions noted.
		CC 6.8-12	Anti-malware programs are installed on all laptops and servers.	**Inquiry**: Inquired of the Endpoint Administrator to determine that anti-malware programs were installed on laptops and servers.	No exceptions noted.
				Observation: Observed the antivirus tool's administration console showing the devices configured with endpoint protection to determine that an anti-malware	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				program was installed on all endpoint devices.	
				Inspection: Inspected the antivirus administration console showing devices not configured with endpoint protection entity devices to determine that there were no laptops or servers connected to the environment without anti-malware installed.	No exceptions noted.
		CC 6.8-13	System administration tasks require the use of a multi-factor authenticated bastion to access consoles.	**Inquiry**: Inquired of the Senior Software Architect to determine that system administration tasks required the use of a multi-factor authenticated Bastion to access consoles.	No exceptions noted.
				Observation: Observed the Senior Software Architect access a production console through the use of a multi-factor authenticated bastion, which required the user to verify the access attempt both using their online account and on their mobile device, to determine that system administration tasks required the use of multi-factor authentication bastion to access consoles.	No exceptions noted.
		CC 6.8-14	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 6: Common Criteria Related to Logical and Physical Access Controls					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 7.1	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.	CC 7.1-01	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 7.1-02	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 7.1-03	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 7.1-04	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry:** Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.1-05	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 7.1-06	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.1-07	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 7.1-08	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 7.2	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.	CC 7.2-01	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 7.2-02	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 7.2-03	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 7.2-04	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.2-05	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 7.2-06	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.2-07	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 7.2-08	Firewall rules for production systems are reviewed and approved by management on a semi-annual basis.	**Inquiry**: Inquired of the Senior IT Risk & Compliance Analyst and the Compliance Auditor to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis.	No exceptions noted.
				Inspection: Inspected the most recent firewall rules review to determine that firewall rules for production systems were reviewed and approved by management on a semi-annual basis, and changes identified were documented and addressed.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.2-09	Software is used to log user activities in Workiva production hosts and the InfoSec team reviews the logs to identify and address unauthorized access to or modification of Workiva production databases.	**Inquiry**: Inquired of the Senior Software Architect to determine that software was used to monitor and alert for unauthorized access to or modification of Workiva production databases, and that alerts were reviewed and addressed.	No exceptions noted.
				Observation: Observed the configuration of the script in the monitoring software to determine that software was used to log user activities in Workiva production databases.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of user activity generated alerts to determine that the InfoSec team reviewed the log of activities to identify and address unauthorized access to or modification of Workiva production databases.	No exceptions noted.
CC 7.3	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.	CC 7.3-01	Workiva has an incident response plan in place to respond to instances of unauthorized use or disclosure of personal information and tests this plan through quarterly exercises.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva had an incident response plan in place to respond to instances of unauthorized use or disclosure of personal information and tested this plan through quarterly exercises.	No exceptions noted.
				Inspection: Inspected the Incident Management Policy to determine that Workiva had an incident response plan in place to respond to instances of unauthorized use or	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				disclosure of personal information.	
				Inspection: Inspected the response plan exercises for a sample of quarters to determine that Workiva tested the plan through quarterly exercises.	No exceptions noted.
		CC 7.3-02	Security incidents are evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	No exceptions noted.
				Inspection: Inspected the Incident Response Procedures document to determine that a policy existed to outline how security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of security incidents tagged as potentially involving customer information or customer data to determine that security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and such information was identified.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.3-03	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 7.3-04	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is configured to log and automatically	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous behavior or processes, and create a ticket for review.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			create a ticket for review.	**Inspection**: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 7.3-05	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 7.3-06	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.3-07	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 7.3-08	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.3-09	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 7.3-10	Members of the Incident Response Team complete annual training to ensure awareness of proper escalation paths and criteria.	**Inquiry**: Inquired of the Senior Director of Information Security and Senior Software Architect to determine that members of the Incident Response Team completed annual training to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
				Inspection: Inspected evidence of completion of Incident Response training for a sample of Incident Response Team members to determine that they completed the training annually to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	CC 7.4-01	Production environments are backed up in full at least weekly. Backup software is configured to alert IT personnel for any backup failure, which is resolved appropriately.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of IT to determine that production environments were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the Google Cloud Platform backup configuration managed by Workiva and the backup process used and managed by Amazon Web Services to determine that production environments were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the Google Cloud Platform backup configuration alerting parameters to determine that backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of backup failures in Google Cloud Platform to determine that backup failures for the Google Cloud Platform were resolved by IT personnel.	No exceptions noted.
		CC 7.4-02	Data restore testing of backup files is	**Inquiry**: Inquired of Senior Director of Information Security to	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			performed at least annually.	determine that data restore testing of backup files was performed at least annually.	
				Inspection: Inspected the ticket for the most recent backup data restore test along with evidence of successful restore to determine that data restore testing of backup files was performed at least annually.	No exceptions noted.
		CC 7.4-03	A Business Continuity and Disaster Recovery Plan has been developed, is documented, is tested annually, and any issues are documented and resolved.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that a Business Continuity and Disaster Recovery Plan was developed, documented, tested annually, and any issues identified were documented and resolved.	No exceptions noted.
				Inspection: Inspected the Business Continuity and Disaster Recovery Plan to determine that it was in place and documented.	No exceptions noted.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that the Business Continuity and Disaster Recovery Plan was tested annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that issues identified were documented and resolved.	The Service Auditor was unable to test the operating effectiveness of this part of the Control Activity as there were no issues identified during the annual Business Continuity and Disaster Recovery test performed during the specified period to which this Control Activity could have been applied.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that there were no issues identified as part of the test.	No exceptions noted.
		CC 7.4-04	Workiva completes an annual Business Continuity exercise, including both a technical and pandemic scenario.	**Inquiry:** Inquired of the Senior Software Architect to determine that Workiva completed an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the evidence of the most recent business continuity exercise to determine that Workiva completed an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.
		CC 7.4-05	The Information Security team performs monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that the Information Security team performed monthly internal assessments to identify, track and resolve critical and high risk vulnerabilities.	No exceptions noted.
				Inspection: Inspected the results of vulnerability assessments for a sample of months to determine that the Information Security team performed monthly internal assessments to identify vulnerabilities.	No exceptions noted.
				Inspection: Inspected the resolution log of vulnerabilities for a sample of months to determine that the Information Security team tracked and resolved critical and high risk vulnerabilities.	No exceptions noted.
		CC 7.4-06	Monitoring software is used to automatically analyze and correlate system information to detect anomalous behavior or processes, and is	**Inquiry**: Inquired of the Senior Software Architect to determine that monitoring software was used to automatically analyze and correlate system information and logs to detect anomalous	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			configured to log and automatically create a ticket for review.	behavior or processes, and create a ticket for review.	
				Inspection: Inspected the configurations of the monitoring software and the ticketing system to determine that a monitoring software was used to automatically analyze and correlate system information to detect anomalous behavior or processes, and was configured to log and automatically create a ticket for review in the ticketing system.	No exceptions noted.
				Inspection: Inspected a sample ticket from the ticketing system to determine that it was created based on an information from the monitoring software.	No exceptions noted.
		CC 7.4-07	Third party penetration and vulnerability testing is performed semi-annually and issues identified are documented and addressed.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that third party penetration and vulnerability testing is performed semi-annually.	No exceptions noted.
				Inspection: Inspected the most recent penetration and vulnerability testing reports conducted by third-party vendors during the reporting period to determine that third-party penetration and vulnerability testing was performed semi-annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the remediation ticket for issues discovered in the third party penetration and vulnerability testing to determine that issues identified were documented and addressed.	No exceptions noted.
		CC 7.4-08	An Intrusion Detection System (IDS) is in place to monitor Workiva's cloud networks continuously for security threats and is configured to alert security incident response personnel when an alarm is triggered. Alerts are logged, tracked, and resolved by security incident response personnel.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an intrusion detection system was in place to monitor Workiva's cloud networks continuously for security threats and was configured to alert security incident response personnel when an alarm was triggered, and that alerts were logged, tracked, and resolved.	No exceptions noted.
				Observation: Observed the Senior Director of Information Security access the Intrusion Detection System to determine that an IDS was in place and that it was configured to alert security incident response personnel when an alarm was triggered by automatically opening a ticket.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of IDS alerts to determine that alerts were logged, tracked, and resolved by security incident response personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.4-09	The organization maintains an Incident Management Policy that addresses the identification, documentation, resolution, communications and escalation of computer security incidences.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that the organization maintained an Incident Management Policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
				Inspection: Inspected the Incident Management Policy to determine that the organization maintained a policy that addressed the identification, documentation, resolution, communications and escalation of computer security incidences.	No exception noted.
		CC 7.4-10	High-severity operational incidents are documented following a root cause analysis, and reviewed by management.	**Inquiry**: Inquired of the Senior Software Architect and the Director of Product Development to determine that high-severity operational incidents were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of high-severity incidents to determine that they were documented following a root cause analysis, and were reviewed by management.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.4-11	An information security, risk and compliance team meets periodically, at least monthly, to review and address security issues.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
				Inspection: Inspected the meeting minutes for a sample of months to determine that an information security, risk and compliance team met periodically, at least monthly, to review and address security issues.	No exceptions noted.
		CC 7.4-12	Workiva has an incident response plan in place to respond to instances of unauthorized use or disclosure of personal information and tests this plan through quarterly exercises.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva had an incident response plan in place to respond to instances of unauthorized use or disclosure of personal information and tested this plan through quarterly exercises.	No exceptions noted.
				Inspection: Inspected the Incident Management Policy to determine that Workiva had an incident response plan in place to respond to instances of unauthorized use or disclosure of personal information.	No exceptions noted.
				Inspection: Inspected the response plan exercises for a sample of quarters to determine that Workiva tested the plan through quarterly exercises.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.4-13	Security incidents are evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	**Inquiry**: Inquired of the Senior Director of Information Technology to determine that security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	No exceptions noted.
				Inspection: Inspected the Incident Response Procedures document to determine that a policy existed to outline how security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and to identify such information.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of security incidents tagged as potentially involving customer information or customer data to determine that security incidents were evaluated to determine whether personal information was used or disclosed inappropriately and such information was identified.	No exceptions noted.
		CC 7.4-14	Members of the Incident Response Team complete annual training to ensure awareness of proper escalation paths and criteria.	**Inquiry**: Inquired of the Senior Director of Information Security and Senior Software Architect to determine that members of the Incident Response Team completed annual training to help ensure awareness	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				of proper escalation paths and criteria.	
				Inspection: Inspected evidence of completion of Incident Response training for a sample of Incident Response Team members to determine that they completed the training annually to help ensure awareness of proper escalation paths and criteria.	No exceptions noted.
CC 7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	CC 7.5-01	The IT Group develops, disseminates, and periodically reviews/updates a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the IT Group developed, disseminated, and periodically reviewed/updated a formal, documented, Security Program Policy that addressed purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.	No exceptions noted.
				Inspection: Inspected the Information Security Policy and the Personnel Security Standard on the Company intranet to determine that the IT Group developed, disseminated, and reviewed/updated annually a formal, documented, Security Program Policy that addresses purpose, scope, roles, responsibilities, management commitment,	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				coordination among organizational entities, and compliance.	
		CC 7.5-02	Production environments are backed up in full at least weekly. Backup software is configured to alert IT personnel for any backup failure, which is resolved appropriately.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of IT to determine that production environments were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the Google Cloud Platform backup configuration managed by Workiva and the backup process used and managed by Amazon Web Services to determine that production environments were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the Google Cloud Platform backup configuration alerting parameters to determine that backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of backup failures in Google Cloud Platform to determine that backup failures for the Google Cloud Platform were resolved by IT personnel.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 7.5-03	Data restore testing of backup files is performed at least annually.	**Inquiry**: Inquired of Senior Director of Information Security to determine that data restore testing of backup files was performed at least annually.	No exceptions noted.
				Inspection: Inspected the ticket for the most recent backup data restore test along with evidence of successful restore to determine that data restore testing of backup files was performed at least annually.	No exceptions noted.
		CC 7.5-04	A Business Continuity and Disaster Recovery Plan has been developed, is documented, is tested annually, and any issues are documented and resolved.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that a Business Continuity and Disaster Recovery Plan was developed, documented, tested annually, and any issues identified were documented and resolved.	No exceptions noted.
				Inspection: Inspected the Business Continuity and Disaster Recovery Plan to determine that it was in place and documented.	No exceptions noted.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that the Business Continuity and Disaster Recovery Plan was tested annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that issues identified were documented and resolved.	The Service Auditor was unable to test the operating effectiveness of this part of the Control Activity as there were no issues identified during the annual Business Continuity and Disaster Recovery test performed during the specified period to which this Control Activity could have been applied.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that there were no issues identified as part of the test.	No exceptions noted.
		CC 7.5-05	Workiva completes an annual Business Continuity exercise, including both a technical and pandemic scenario.	**Inquiry**: Inquired of the Senior Software Architect to determine that Workiva completed an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 7: Common Criteria Related to Systems Operations					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the evidence of the latest business continuity exercise to determine that Workiva completes an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	CC 8.1-01	System Development Life Cycle policies and procedures are in place.	**Inquiry**: Inquired of the Senior Software Architect to determine that System Development Life Cycle policies and procedures were in place.	No exceptions noted.
				Inspection: Inspected the Application Security Standard to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
				Inspection: Inspected the Development Security Review procedure and the SDLC process flow chart to determine that the System Development Life Cycle policies and procedures were in place.	No exceptions noted.
		CC 8.1-02	Quality assurance testing procedures are performed and documented for code changes to the production environment.	**Inquiry**: Inquired of the Senior Software Architect to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases to determine that quality assurance testing procedures were performed and documented for code changes to the production environment.	No exceptions noted.
		CC 8.1-03	Separate Test, Development, and Production environments are	**Inquiry**: Inquired of the Senior Software Architect to determine that separate test, development, and production environments	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			maintained for the Workiva platform.	were maintained for the Workiva platform.	
				Observation: Observed the test, development and production environments for the Workiva platform to determine that separate environments were maintained.	No exceptions noted.
		CC 8.1-04	System changes that can impact the security of the system have security reviews performed and signed off by management prior to release into production.	**Inquiry**: Inquired of the Senior Software Architect to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
				Inspection: Inspected the Development Security Guidelines to determine that they documented the process around the security reviews performed for system changes impacting the security of the system.	No exceptions noted.
				Inspection: Inspected the evidence of security review and sign off for a sample of changes to determine that system changes that can impact the security of the system had security reviews performed and signed off by management prior to release into production.	No exceptions noted.
		CC 8.1-05	Release Management verifies Development and Quality Assurance requirements have been met prior to	**Inquiry**: Inquired of the Senior Software Architect to determine that Release Management verified Development and Quality Assurance requirements	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			release into production.	were met prior to release into production.	
				Observation: Observed the automated process to release changes to production to determine that release management verified development and quality assurance requirements were met prior to releasing the change into production and halted the release when certain requirements were not met.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of releases to determine that Release Management verified Development and Quality Assurance requirements were met prior to release into production.	No exceptions noted.
		CC 8.1-06	Segregation of responsibilities for code changes to the production environment is maintained between development, code review, and release processes.	**Inquiry**: Inquired of the Senior Software Architect to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
				Inspection: Inspected the System Development Life Cycle process flow chart to determine that segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the ticket for a sample of releases showing the individuals who performed code review and QA review and the automated release tool that pushed the release to production to determine that separate individuals performed code review, QA review, and release signoff showing segregation of responsibilities for code changes to the production environment was maintained between development, code review, and release processes.	No exceptions noted.
		CC 8.1-07	Starting June 2019, static code analysis is performed monthly. Issues identified are triaged and remediated according to Workiva's documented remediation timelines.	**Inquiry**: Inquired of the Director of Information Security to determine that starting June 2019, static code analysis was performed monthly and that issues identified were triaged and remediated according to Workiva's documented remediation timelines.	No exceptions noted.
				Inspection: Inspected the results of the static code analysis performed for a sample of months since June 2019 to determine that static code analysis was performed monthly and issues identified were triaged and remediated.	No exceptions noted.
				Inspection: Inspected the results of the static code analysis performed for a sample of months	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				since June 2019 to determine that there were no issues identified.	
		CC 8.1-08	Version control software is in place to manage current versions of source code for the in-scope applications. The ability to modify source code for the in-scope applications is restricted to appropriate personnel based on job function.	**Inquiry**: Inquired of the Senior Software Architect to determine that version control software was in place to manage current versions of source code for the in-scope applications and the ability to modify source code for the in-scope applications was restricted to appropriate personnel based on job function.	No exceptions noted.
				Observation: Observed the Senior Software Architect attempt to merge a change into production without appropriate Release Management approval and the change being blocked from release to production to determine that the ability to modify source code for the in-scope application was restricted appropriately.	No exceptions noted.
				Inspection: Inspected the list of users with access to modify source code and their job responsibilities to determine that the ability was restricted appropriately.	No exceptions noted.
		CC 8.1-09	Workiva policy requires confidential data to be de-identified prior to use in testing or movement into other non-	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Workiva policy required confidential data to be de-identified prior to use in	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			production environments.	testing or movement into other non-production environments.	
				Observation: Observed the Senior Director of Information Security access data within the test environment to determine that the data was sanitized, and confirmed that Workiva de-identified data according to policy prior to use in testing or movement into other non-production environments.	No exceptions noted.
				Inspection: Inspected the Application Development Policy to determine that Workiva policy required confidential data to be de-identified prior to use in testing or movement into other non-production environments.	No exceptions noted.
		CC 8.1-10	Configuration hardening guidelines are documented to define the configuration of production systems.	**Inquiry**: Inquired of the Senior Software Architect to determine that configuration hardening guidelines were documented to define the configuration of production systems.	No exceptions noted.
				Observation: Observed the script file used to configure production systems on a sample system to determine that configuration hardening guidelines were defined for the configuration of production systems.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 8: Common Criteria Related to Change Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the configuration hardening guidelines to determine that such guidelines were documented to define the configuration of production systems.	No exceptions noted.
		CC 8.1-11	Production systems are kept in conformance to hardening guidelines through the use of continuous compliance scanning.	**Inquiry**: Inquired of the Senior Software Architect to determine that production systems were kept in conformance to hardening guidelines through the use of continuous compliance scanning.	No exceptions noted.
				Observation: Observed the configuration of the entity's production host monitoring tool to determine that it scanned production systems to verify they were in conformance to hardening guidelines, and generated an alert when systems were identified as being in compliance with guidelines.	No exceptions noted.
				Inspection: Inspected the log of alerts resulting from the continuous compliance scanning along with the resolution status to determine that production systems were scanned for conformance with hardening guidelines, and that alerts were auto-generated by the tool when changes were made that led to non-conformance and addressed.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	CC 9.1-01	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 9.1-02	Production environments are backed up in full at least weekly. Backup software is configured to alert IT personnel for any backup failure, which is resolved appropriately.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of IT to determine that production environments were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the Google Cloud Platform backup configuration managed by Workiva and the backup process used and managed by Amazon Web Services to determine that production environments	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				were backed up in full at least weekly and backup software was configured to alert IT personnel for any backup failure.	
				Inspection: Inspected the Google Cloud Platform backup configuration alerting parameters to determine that backup software was configured to alert IT personnel for any backup failure.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of backup failures in Google Cloud Platform to determine that backup failures for the Google Cloud Platform were resolved by IT personnel.	No exceptions noted.
		CC 9.1-03	Data restore testing of backup files is performed at least annually.	**Inquiry**: Inquired of Senior Director of Information Security to determine that data restore testing of backup files was performed at least annually.	No exceptions noted.
				Inspection: Inspected the ticket for the most recent backup data restore test along with evidence of successful restore to determine that data restore testing of backup files was performed at least annually.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
		CC 9.1-03	A Business Continuity and Disaster Recovery Plan has been developed, is documented, is tested annually, and any issues are documented and resolved.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that a Business Continuity and Disaster Recovery Plan was developed, documented, tested annually, and any issues identified were documented and resolved.	No exceptions noted.
				Inspection: Inspected the Business Continuity and Disaster Recovery Plan to determine that it was in place and documented.	No exceptions noted.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that the Business Continuity and Disaster Recovery Plan was tested annually.	No exceptions noted.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that issues identified were documented and resolved.	The Service Auditor was unable to test the operating effectiveness of this part of the Control Activity as there were no issues identified during the annual Business Continuity and Disaster Recovery test performed

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
					during the specified period to which this Control Activity could have been applied.
				Inspection: Inspected the most recent Business Continuity and Disaster Recovery test results to determine that there were no issues identified as part of the test.	No exceptions noted.
		CC 9.1-04	Workiva completes an annual Business Continuity exercise, including both a technical and pandemic scenario.	**Inquiry**: Inquired of the Senior Software Architect to determine that Workiva completed an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.
				Inspection: Inspected the evidence of the latest business continuity exercise to determine that Workiva completes an annual Business Continuity exercise, including both a technical and pandemic scenario.	No exceptions noted.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	CC 9.2-01	Security incident response procedures are documented to guide employees in identifying, reporting, and acting upon security incidents.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that security incident response procedures were documented to guide employees in identifying, reporting, and acting upon security incidents.	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Security Incident Response Procedure to determine that procedures were documented to guide employees in identifying, reporting, and acting upon security incidents.	No exceptions noted.
		CC 9.2-02	An annual risk assessment review is conducted on vendors providing mission critical services in support of the production environment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that an annual risk assessment review was conducted on vendors providing mission critical services in support of the production environment.	No exceptions noted.
				Inspection: Inspected the most recent reviews to determine that an annual risk assessment review was conducted of vendors providing mission critical services in support of the production environment.	No exceptions noted.
		CC 9.2-03	Management performs a risk assessment of the off-site data centers on an annual basis, including verification of ISO 27001 certification or an in-person assessment.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that management performed a risk assessment of the off-site data centers, including verification of ISO 27001 certification or in-person assessment.	No exceptions noted.
				Inspection: Inspected the risk assessment performed, including the review of the ISO certification, for off-site data center providers to determine that management performed a risk assessment of the off-site data centers, including	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				verification of ISO 27001 certification.	
		CC 9.2-04	Workiva's security and confidentiality commitments regarding the system are included in the master services agreement and customer-specific service level agreements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		CC 9.2-05	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				security and confidentiality requirements.	
		CC 9.2-06	An annual risk assessment and business impact analysis is conducted to evaluate risks to the Workiva platform environment and help ensure appropriateness of controls.	**Inquiry**: Inquired of Senior Director of Information Security to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
				Inspection: Inspected the most current Business Risk Assessment to determine that an annual risk assessment and business impact analysis was conducted to evaluate risks to the Workiva platform environment and to help ensure appropriateness of controls.	No exceptions noted.
		CC 9.2-07	The Information Security team performs monthly internal reviews to assess compliance with information security policies.	**Inquiry**: Inquired of the Senior Director of Information Security and the VP of Information Technology to determine that the Information Security team performed monthly internal reviews to assess compliance with information security policies.	No exceptions noted.
				Inspection: Inspected the internal compliance review performed for a sample of months to determine that the Information Security team performed monthly internal reviews to assess	No exceptions noted.

COMMON CRITERIA PRINCIPLE: Criteria Common to the Security and Confidentiality Trust Services Categories					
CRITERIA GROUP 9: Common Criteria Related to Risk Management					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				compliance with information security policies.	

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
C 1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.	C 1.1-01	The Compliance Officer maintains, approves and publishes a Customer Confidentiality & Securities Trading Policy.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that the Compliance Officer maintained, approved and published a Customer Confidentiality & Securities Trading Policy.	No exceptions noted.
				Inspection: Inspected the Customer Confidentiality & Securities Policy to determine that the Compliance Officer maintained, approved and published a policy around confidentiality and securities trading.	No exceptions noted.
		C 1.1-02	Employees and contractors are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	**Inquiry:** Inquired of the VP of HR to determine that employees and contractors were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.
				Inspection: Inspected the signed confidentiality agreements for a sample of employees and contractors to determine that they were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.
		C 1.1-03	Workiva's security and confidentiality commitments regarding the system are included in the master services	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that Workiva's security and confidentiality commitments regarding	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
			agreement and customer-specific service level agreements.	the system were included in the master services agreement and customer-specific service level agreements.	
				Inspection: Inspected the agreement for a sample of clients to determine that Workiva's security and confidentiality commitments regarding the system were included in the master services agreement and customer-specific service level agreements.	No exceptions noted.
		C 1.1-04	Agreements with sub-processors of Restricted-level customer information include language to address security and confidentiality requirements.	**Inquiry**: Inquired of the EVP Chief Legal Officer to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
				Inspection: Inspected the service agreements with third-parties, including Google, and AWS to determine that agreements with sub-processors of Restricted-level customer information included language to address security and confidentiality requirements.	No exceptions noted.
		C 1.1-05	Customer data is encrypted at rest using AES256 encryption.	**Inquiry**: Inquired of the Senior Software Architect to determine that customer data was encrypted at rest using AES-256 encryption.	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
				Inspection: Inspected the encryption configuration for the Google Cloud Platform managed by Workiva and the native encryption method used and managed by Amazon Web Services to determine customer data was encrypted using AES-256 encryption.	No exceptions noted.
				Inspection: Inspected a sample client's data within Google Cloud to determine that customer data was encrypted using AES-256 encryption.	No exceptions noted.
		C 1.1-06	A Data Classification policy is in place and defines handling procedures for each level of classification.	**Inquiry**: Inquired of the Director of Information Security to determine that a Data Classification policy was in place and defined handling procedures for each level of classification.	No exceptions noted.
				Inspection: Inspected the Data Classification Policy to determine that a policy was in place and defined handling procedures for each level of classification.	No exceptions noted.
		C 1.1-07	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
C 1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.	C 1.2-01	A process is in place to destroy customer data when requested by the customer.	**Inquiry**: Inquired of the VP of IT and Senior Director of Information Security to determine that a process was in place to destroy customer data when requested by the customer.	No exceptions noted.
				Inspection: Inspected the ticket for a sample of customer data destruction requests to determine that a process was in place to destroy customer data upon request.	No exceptions noted.
		C 1.2-02	Equipment that has stored non-public information must be sanitized in accordance with the Equipment Disposal Procedure before it can be disposed of or used for other purposes (including internal and removable media).	**Inquiry**: Inquired of the Senior Software Architect to determine that equipment that has stored non-public information was sanitized in accordance with the Equipment Disposal Procedure before it was disposed of or re-used.	No exceptions noted.
				Observation: Observed the process of wiping a machine after use to determine that equipment that has stored non-public information was sanitized in accordance with the Equipment Disposal Procedure before it was disposed of or re-used.	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
				Inspection: Inspected the Equipment Disposal Procedure to determine that a baseline procedure was in place for sanitization of equipment that had stored non-public information.	No exceptions noted.
				Inspection: Inspected the disposal documentation for a sample of decommissioned equipment to determine that the equipment was sanitized in accordance with the Equipment Disposal Procedure prior to disposal.	No exceptions noted.
		C 1.2-03	Mobile Device Management software is deployed to protect mobile devices that serve as information assets.	**Inquiry**: Inquired of the Senior Director of Information Security to determine that Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
				Inspection: Inspected the configuration of the Mobile Management to determine that a Mobile Device Management software was deployed to protect mobile devices that served as information assets.	No exceptions noted.
		C 1.2-04	Paper containing confidential information is destroyed by shredding or by placing in a designated shredding receptacle. Destruction is	**Inquiry**: Inquired of the Chief Administration Officer to determine that paper containing confidential information was destroyed by shredding or by placing in a designated shredding receptacle and that	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		**Control Activity Number**	**Control Activity Description**	**Tests Performed By Service Auditor**	**Results of Testing**
			validated through the receipt of a certificate of destruction.	destruction was validated through the receipt of a certificate of destruction.	
				Observation: Observed the shred bins throughout the headquarters to determine that shredding receptacles were made available to dispose of paper containing confidential information.	No exceptions noted.
				Inspection: Inspected the Information Asset Management Policy and the agreement with the shredding vendor to determine that a process and vendor were in place to destroy items disposed off in the shredding receptacle.	No exceptions noted.
				Inspection: Inspected the certificate of destruction for a sample of months to determine that destruction of confidential information placed in shredding receptacles was validated through the receipt of a certificate of destruction.	No exceptions noted.
		C 1.2-05	Employees and contractors are required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information,	**Inquiry:** Inquired of the VP of HR to determine that employees and contractors were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.

CONFIDENTIALITY CRITERIA: Additional Criteria for Confidentiality					
CRITERIA GROUP 1: Additional Criteria for Confidentiality					
Applicable Trust Services Criteria		Control Activity Number	Control Activity Description	Tests Performed By Service Auditor	Results of Testing
			including client information.	**Inspection:** Inspected the signed confidentiality agreements for a sample of employees and contractors to determine that they were required to sign a confidentiality statement agreeing not to disclose proprietary or confidential information, including client information.	No exceptions noted.

V. Other Information Provided by Workiva, Inc.

The information in this section is presented by the Company to provide additional information to its user entities, business partners, and other specified parties and is not part of the Company's description of its system and controls included in Section III. The information in Section A, "HIPAA Mapping to SOC 2 Controls" has not been subjected to the procedures applied in the examination of the description of the Company's Cloud-Based Collaboration Solutions and Support Operations and suitability of design and operating effectiveness of controls to achieve the Company's service commitments and system requirements based on the applicable trust services criteria, and accordingly, Grant Thornton LLP expresses no opinion on it.

A. HIPAA Mapping to SOC 2 Controls

The security practices defined by Workiva management, based on the aforementioned Security trust services principles, are relevant to and support certain elements of the Health Insurance Portability and Accountability Act of 1996 ("HIPAA") Security and Privacy rules. HIPAA controls relevant to security have been mapped below to the corresponding SOC 2 security controls to help readers interpret the results of testing in Section IV to HIPAA.

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.308(a)(1)(i)	Standard: Security management process. Implement policies and procedures to prevent, detect, contain, and correct security violations.	CC 1.1-04 CC 1.1-10 CC 1.1-11
164.308(a)(1)(ii)(B)	Risk management. Implement security measures sufficient to reduce risks and vulnerabilities to a reasonable and appropriate level to comply with §164.306(a).	
164.308(a)(2)	Standard: Assigned security responsibility. Identify the security official who is responsible for the development and implementation of the policies and procedures required by this subpart for the covered entity or business associate.	
164.316(a)	Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.316(b)(1)(i)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	CC 1.1-04 CC 1.1-10 CC 1.1-11 (continued)
164.316(b)(1)(ii)	If an action, activity or assessment is required by this subpart to be documented, maintain a written (which may be electronic) record of the action, activity, or assessment.	
164.316(b)(2)(i)	Time limit. Retain the documentation required by paragraph (b)(1) of this section for 6 years from the date of its creation or the date when it last was in effect, whichever is later.	
164.316(b)(2)(ii)	Make documentation available to those persons responsible for implementing the procedures to which the documentation pertains.	
164.316(b)(2)(iii)	Review documentation periodically, and update as needed, in response to environmental or operational changes affecting the security of the electronic protected health information.	
164.308(a)(5)(ii)(A)	Periodic security updates.	CC 1.1-11 CC 2.2-08 CC 9.2-01
164.308(a)(6)(i)	Standard: Security incident procedures. Implement policies and procedures to address security incidents.	
164.316(a)	Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	
164.316(b)(1)(i)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	
164.312(a)(2)(ii)	Establish (and implement as needed) procedures for obtaining necessary electronic protected health information during an emergency.	CC 2.2-07 CC 2.2-12
164.308(a)(5)(i)	Standard: Security awareness and training. Implement a security awareness and training program for all members of its workforce (including management).	

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.308(a)(5)(ii)(A)	Periodic security updates.	CC 1.1-11 CC 2.3-04 CC 2.3-05
164.308(a)(6)(i)	Standard: Security incident procedures. Implement policies and procedures to address security incidents.	
164.316(a)	Standard: Policies and procedures. Implement reasonable and appropriate policies and procedures to comply with the standards, implementation specifications, or other requirements of this subpart, taking into account those factors specified in §164.306(b)(2)(i), (ii), (iii), and (iv). This standard is not to be construed to permit or excuse an action that violates any other standard, implementation specification, or other requirements of this subpart. A covered entity or business associate may change its policies and procedures at any time, provided that the changes are documented and are implemented in accordance with this subpart.	
164.316(b)(1)(i)	Maintain the policies and procedures implemented to comply with this subpart in written (which may be electronic) form; and	
164.308(a)(1)(ii)(A)	Risk analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	CC 3.2-01 CC 3.3-05
164.308(a)(7)(ii)(E)	Applications and data criticality analysis. Assess the relative criticality of specific applications and data in support of other contingency plan components.	CC 3.2-01 CC 3.3-05
164.308(a)(1)(ii)(D)	Information system activity review. Implement procedures to regularly review records of information system activity, such as audit logs, access reports, and security incident tracking reports.	CC 2.1-04 CC 3.2-08 CC 4.1-07
164.308(a)(5)(ii)(C)	Log-in monitoring. Procedures for monitoring log-in attempts and reporting discrepancies.	
164.312(b)	Standard: Audit controls. Implement hardware, software, and/or procedural mechanisms that record and examine activity in information systems that contain or use electronic protected health information.	
164.308(a)(1)(ii)(A)	Risk analysis. Conduct an accurate and thorough assessment of the potential risks and vulnerabilities to the confidentiality, integrity, and availability of electronic protected health information held by the covered entity or business associate.	CC 5.2-12 CC 5.1-10 CC 5.1-09 CC 7.4-04
164.308(a)(7)(ii)(D)	Testing and revision procedures. Implement procedures for periodic testing and revision of contingency plans.	
164.308(a)(8)	Standard: Evaluation. Perform a periodic technical and nontechnical evaluation, based initially upon the standards implemented under this rule and, subsequently, in response to environmental or operational changes affecting the security of electronic protected health information, that establishes the extent to which a covered entity's or business associate's security policies and procedures meet the requirements of this subpart.	

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.308(a)(4)(ii)(B)	Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	CC 5.2-01 CC 5.2-03 CC 5.2-08
164.312(a)(2)(i)	Unique user identification. Assign a unique name and/or number for identifying and tracking user identity.	
164.312(d)	Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	
164.308(a)(5)(ii)(D)	Password management. Procedures for creating, changing, and safeguarding passwords.	
164.308(a)(3)(ii)(A)	Authorization and/or supervision. Implement procedures for the authorization and/or supervision of workforce members who work with electronic protected health information or in locations where it might be accessed.	CC 6.2-01 CC 6.2-03
164.308(a)(3)(ii)(C)	Termination procedures. Implement procedures for terminating access to electronic protected health information when the employment of, or other arrangement with, a workforce member ends or as required by determinations made as specified in paragraph (a)(3)(ii)(B) of this section.	
164.308(a)(4)(i)	Standard: Information access management. Implement policies and procedures for authorizing access to electronic protected health information that are consistent with the applicable requirements of subpart E of this part.	
164.308(a)(4)(ii)(C)	Access establishment and modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	
164.308(a)(4)(ii)(B)	Access authorization. Implement policies and procedures for granting access to electronic protected health information, for example, through access to a workstation, transaction, program, process, or other mechanism.	CC 5.2-04 CC 5.2-08 CC 6.1-09
164.312(a)(2)(iii)	Automatic logoff. Implement electronic procedures that terminate an electronic session after a predetermined time of inactivity.	
164.312(d)	Standard: Person or entity authentication. Implement procedures to verify that a person or entity seeking access to electronic protected health information is the one claimed.	
164.308(a)(3)(ii)(B)	Workforce clearance procedure. Implement procedures to determine that the access of a workforce member to electronic protected health information is appropriate.	CC 6.3-06
164.308(a)(4)(ii)(C)	Access establishment and modification. Implement policies and procedures that, based upon the covered entity's or the business associate's access authorization policies, establish, document, review, and modify a user's right of access to a workstation, transaction, program, or process.	

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.310(a)(1)	Standard: Facility access controls. Implement policies and procedures to limit physical access to its electronic information systems and the facility or facilities in which they are housed, while ensuring that properly authorized access is allowed.	CC 6.4-06 CC 6.4-07 CC 6.4-01 CC 6.4-03
164.310(a)(2)(ii)	Facility security plan. Implement policies and procedures to safeguard the facility and the equipment therein from unauthorized physical access, tampering, and theft.	
164.310(a)(2)(iii)	Access control and validation procedures. Implement procedures to control and validate a person's access to facilities based on their role or function, including visitor control, and control of access to software programs for testing and revision.	
164.310(b)	Standard: Workstation use. Implement policies and procedures that specify the proper functions to be performed, the manner in which those functions are to be performed, and the physical attributes of the surroundings of a specific workstation or class of workstation that can access electronic protected health information.	CC 6.7-15 CC 6.7-10 CC 6.7-16 CC 5.2-20
164.310(c)	Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	
164.310(d)(1)	Standard: Device and media controls. Implement policies and procedures that govern the receipt and removal of hardware and electronic media that contain electronic protected health information into and out of a facility, and the movement of these items within the facility.	
164.312(a)(2)(iv)	Encryption and decryption. Implement a mechanism to encrypt and decrypt electronic protected health information.	
164.312(c)(1)	Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	
164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	
164.312(e)(1)	Standard: Transmission security. Implement technical security measures to guard against unauthorized access to electronic protected health information that is being transmitted over an electronic communications network.	
164.312(e)(2)(i)	Integrity controls. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
164.312(e)(2)(ii)	Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	
164.308(a)(5)(ii)(B)	Protection from malicious software. Procedures for guarding against, detecting, and reporting malicious software.	CC 6.8-12

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.308(a)(7)(i)	Standard: Contingency plan. Establish (and implement as needed) policies and procedures for responding to an emergency or other occurrence (for example, fire, vandalism, system failure, and natural disaster) that damages systems that contain electronic protected health information.	CC 7.2-05
164.308(a)(7)(ii)(B)	Disaster recovery plan. Establish (and implement as needed) procedures to restore any loss of data.	
164.308(a)(7)(ii)(C)	Emergency mode operation plan . Establish (and implement as needed) procedures to enable continuation of critical business processes for protection of the security of electronic protected health information while operating in emergency mode.	
164.310(a)(2)(i)	Contingency operations. Establish (and implement as needed) procedures that allow facility access in support of restoration of lost data under the disaster recovery plan and emergency mode operations plan in the event of an emergency.	
164.308(a)(1)(ii)(C)	Sanction policy. Apply appropriate sanctions against workforce members who fail to comply with the security policies and procedures of the covered entity or business associate.	CC 1.1-06 CC 7.2-06
164.308(a)(6)(ii)	Implementation specification: Response and reporting. Identify and respond to suspected or known security incidents; mitigate, to the extent practicable, harmful effects of security incidents that are known to the covered entity or business associate; and document security incidents and their outcomes.	CC 8.1-01
164.308(a)(3)(i)	Standard: Workforce security. Implement policies and procedures to ensure that all members of its workforce have appropriate access to electronic protected health information, as provided under paragraph (a)(4) of this section, and to prevent those workforce members who do not have access under paragraph (a)(4) of this section from obtaining access to electronic protected health information.	CC 5.2-17 CC 6.1-11
164.308(a)(4)(ii)(A)	Isolating health care clearinghouse functions. If a health care clearinghouse is part of a larger organization, the clearinghouse must implement policies and procedures that protect the electronic protected health information of the clearinghouse from unauthorized access by the larger organization.	
164.310(d)(2)(i)	Disposal. Implement policies and procedures to address the final disposition of electronic protected health information, and/or the hardware or electronic media on which it is stored.	
164.310(d)(2)(ii)	Media re-use. Implement procedures for removal of electronic protected health information from electronic media before the media are made available for re-use.	
164.310(d)(2)(iii)	Accountability. Maintain a record of the movements of hardware and electronic media and any person responsible therefore.	
164.312(a)(1)	Standard: Access control. Implement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights as specified in §164.308(a)(4).	

HIPAA Element	HIPAA Security Rule Reference	Related Workiva Control #
164.312(a)(2)(iv)	Encryption and decryption. Implement a mechanism to encrypt and decrypt electronic protected health information.	CC 6.1-06 CC 6.6-11
164.312(c)(1)	Standard: Integrity. Implement policies and procedures to protect electronic protected health information from improper alteration or destruction.	
164.312(c)(2)	Implementation specification: Mechanism to authenticate electronic protected health information. Implement electronic mechanisms to corroborate that electronic protected health information has not been altered or destroyed in an unauthorized manner.	
164.312(e)(2)(i)	Integrity controls. Implement security measures to ensure that electronically transmitted electronic protected health information is not improperly modified without detection until disposed of.	
164.312(e)(2)(ii)	Encryption. Implement a mechanism to encrypt electronic protected health information whenever deemed appropriate.	
164.308(b)(1)	Business associate contracts and other arrangements. A covered entity may permit a business associate to create, receive, maintain, or transmit electronic protected health information on the covered entity's behalf only if the covered entity obtains satisfactory assurances, in accordance with §164.314(a), that the business associate will appropriately safeguard the information. A covered entity is not required to obtain such satisfactory assurances from a business associate that is a subcontractor.	CC 6.5-02 CC 6.5-03 CC 9.2-05
164.308(b)(4)	Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	
164.314(a)(1)(i)	Business associate contracts or other arrangements. The contract or other arrangement between the covered entity and its business associate required by §164.308(b) must meet the requirements of paragraph (a)(2)(i) or (a)(2)(ii) of this section, as applicable.	
164.314(a)(2)(i)(A)	Comply with the applicable requirements of this subpart;	
164.314(a)(2)(i)(B)	In accordance with §164.308(b)(2), ensure that any subcontractors that create, receive, maintain, or transmit electronic protected health information on behalf of the business associate agree to comply with the applicable requirements of this subpart by entering into a contract or other arrangement that complies with this section;	
164.314(a)(2)(i)(C)	Report to the covered entity any security incident of which it becomes aware, including breaches of unsecured protected health information as required by § 164.410.	
164.314(a)(2)(ii)	Other arrangements. The covered entity is in compliance with paragraph (a)(1) of this section if it has another arrangement in place that meets the requirements of §164.504(e)(3).	
164.314(a)(2)(iii)	Business associate contracts with subcontractors. The requirements of paragraphs (a)(2)(i) and (a)(2)(ii) of this section apply to the contract or other arrangement between a business associate and a subcontractor required by §164.308(b)(4) in the same manner as such requirements apply to contracts or other arrangements between a covered entity and business associate.	

ADDENDUM ACKNOWLEDGEMENT FORM
SOLICITATION NO.: FAR2000000002

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)

[✓] 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 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.

Vertosoft LLC
Company

Clint Hayes
Authorized Signature

2/13/2020
Date

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

Master Terms and Conditions USVN08122019

BY CLICKING A BOX INDICATING YOUR ACCEPTANCE OR BY SIGNING AN ORDER REFERENCING THESE MASTER TERMS AND CONDITIONS (INCLUDING ALL REFERENCED DOCUMENTS OR LINKS HEREIN, THE "MASTER TERMS AND CONDITIONS" AND ALONG WITH ALL ORDERS, THE "AGREEMENT") ON BEHALF OF THE COMPANY SET FORTH IN SUCH ORDER THE SIGNER IS HEREBY ENTERING INTO THE MASTER TERMS AND CONDITIONS AND THE AGREEMENT ON BEHALF OF SUCH COMPANY (THE "CUSTOMER") WITH THE WORKIVA ENTITY ALSO NAMED IN SUCH ORDER ("WORKIVA"). IN DOING SO THE SIGNER REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO BIND CUSTOMER AND ITS AFFILIATES TO THESE MASTER TERMS AND CONDITIONS AND THE AGREEMENT.

1.0 Services. Subscription Services and Professional Services (collectively referred to herein as, the "Services") are each available for Customer as set forth in these Master Terms and Conditions and the applicable ordering document (in the case of Subscription Services, a "Subscription Order," in the case of Professional Services, a "Services Order," "Statement of Work," or a "SOW," and for purposes of the Agreement, these ordering documents may be collectively referred to as, "Orders" or individually as, an "Order") entered into by Workiva and Customer.

1.1 Professional Services. Workiva shall provide professional Services such as setups, trainings, and other professional services ("Professional Services") as set forth in the applicable Services Order. Customer agrees to the Professional Services terms found here www.workiva.com/professionalserviceaddendum which will apply to Workiva's provision of Professional Services.

1.2 Subscription Services.

(a) Pursuant to the terms of the Agreement, Workiva shall provide Customer with subscription based access, exercisable through Customer's Users (defined below), to the Software (the "Subscription Services"). The Subscription Services include Software related support as set forth in the Subscription Order ("Support"). "Software" means Workiva's cloud based software programs which are made up of Workiva's proprietary software and applicable Third Party Software (as the case may be), as more adequately described in the applicable Subscription Order, and the Documentation. "Documentation" means the manuals, specifications, and other materials describing the functionality, features, and operating characteristics of the Software, available at https://success.wdesk.com/help, including any updates thereto. "Third Party Software" means software and services authored by a third party, including, the Google App Engine and Amazon Web Services.

(b) During the Subscription Term, subject to the terms of the Agreement, Workiva grants to Customer and its Users, a non-exclusive, non-transferable, worldwide right and license to access, use, and display the Software in connection with the Subscription Services. “Users” means employees of Customer or Named Affiliates that are provided with (or that Workiva provides at Customer’s request) user identifications and passwords to Customer’s account. Users may include consultants, contractors, agents, and third parties with which Customer transacts business. For the avoidance of doubt, Users must be human. Users registered as, or by, “bots” or other automated methods, are not permitted. Accordingly, Workiva reserves the right to suspend any such Users without notice to Customer. Users will be determined on a named user basis rather than on a concurrent user or shared user basis; provided that Customer may reassign different individuals on a reasonable basis (e.g., an employee changes positions or leaves Customer’s employ). Customer is responsible for each of its Users’ acts and omissions and remains liable to Workiva for any User’s (including an authorized third party acting as a User on Customer’s behalf) breach of the Agreement.

(c) Over the course of the Agreement Term Workiva may, in its sole discretion, update features, functionality, software, or user types that Customer accesses pursuant to an active Order; provided that such updates will be at no cost to Customer and will not materially degrade existing features and functionality. Accordingly, Workiva reserves the right to update Customer’s Software accordingly so that it remains current with the then current version of Software available to Workiva’s customers generally. In addition, Workiva may release new features, functionality, software, or user types that are only available under a different pricing model or on a version of Software other than the version Customer currently accesses. In the event Customer desires to purchase any new features Workiva reserves the right, in its sole discretion, to update Customer’s account, pricing model, or Software version to facilitate the provision of such new features.

1.3 Services to Customer Affiliates.

(a) “Affiliate” means any corporation, partnership, joint venture, joint stock company, limited liability company, trust, estate, association, or other entity the existence of which is recognized by any governmental authority, (collectively an “Entity”) that directly or indirectly through one or more intermediaries, controls or is controlled by or is under common control with either Customer or Workiva or any Entity in which Customer or Workiva has any direct or indirect ownership interest, whether controlling or not, of at least 50%, at any time during the Agreement Term (defined in Section 4.1 below). For purposes of this definition the term “controls”, “is controlled by” or “under common control with” means the possession, direct or indirect, of the power to direct or cause the direction of the management and policies of such entity, whether through the ownership of voting securities, by contract or otherwise.

(b) Customer may only permit Affiliates named in an Order (“Named Affiliate”), and such Affiliates’ employees, to access the Software pursuant to Customer’s Agreement

(in contrast to accessing the Software pursuant to such Affiliate's own Agreement). Customer will be responsible for any Named Affiliate's, or its Users', compliance with the terms of the Agreement and, for purposes of the foregoing, all obligations of Customer shall apply equally to each such Named Affiliate that receives Services under a Customer Order.

2.0 Security; Customer Data.

2.1 Security. As a part of the Services Workiva shall maintain appropriate administrative, physical, and technical safeguards for the security, confidentiality and integrity of any data or information inputted, edited, authored, generated, managed, or otherwise submitted by Customer or its Users into Customer's subscription account ("Customer Data"), as described in Workiva's Security standards set forth here www.workiva.com/securityrequirements_3.0 ("Security Standards"). The Security Standards shall be deemed compliant with Workiva's obligations to protect Customer Data as set forth in the Agreement. To the extent Customer Data includes personal data, Workiva represents and warrants to only process such data pursuant to Customer's requests or as otherwise set forth in the Data Processing Agreement as set forth here www.workiva.com/dataprocessingagreement_1.0 (the "Data Processing Agreement" or "DPA").

2.2 Customer Data; Other Responsibilities. Workiva shall not modify, disclose (except as compelled by law in accordance with Section 5.4, to perform Services or as expressly permitted in writing by Customer), or access (except to provide or improve the Software or Services and prevent or address service or technical problems, or at Customer's request in connection with Support) Customer Data. Workiva and its service providers may not otherwise collect, use, disclose, or utilize Customer Data. Workiva shall provide the Services in accordance with applicable laws and government regulations. Except as otherwise agreed in writing and subject to Workiva's warranties set forth herein, (a) Customer is responsible for the accuracy, truthfulness, consistency, completeness, and any output from the Software, and (b) Workiva will neither have the responsibility to review, nor any liability as to the accuracy of, any information or content posted by Customer or its Users. Customer is responsible for any consents necessary for the collection, use and disclosure of all Customer Data in accordance with the Agreement. Customer's and its Users' use of the Software will comply with applicable local, state, federal and international law, regulations and conventions, including without limitation those related to data privacy, international communications, and the exportation of technical or personal data. Customer represents and warrants to Workiva that Customer has sufficient rights in the Customer Data to authorize Workiva to collect, use, disclose, process, distribute and display the Customer Data as contemplated by the Agreement, and that the Customer Data and its use hereunder will not violate or infringe the rights of any third party. The security, deletion, correction, accuracy, quality, integrity, legality, reliability, appropriateness, intellectual property ownership in, or right to use any Customer Data transmitted, exported, or sent from the Software to any third party software environment or system, shall be solely subject to the terms of Customer's

agreement with such third party and Workiva will have no responsibility for Customer's use of, or Customer Data stored or residing on, such third party software environment or system and the terms of this Agreement will not apply.

2.3 Web Analytics. In providing the Services, Workiva utilizes the services of Google and Amazon ("Cloud Hosting Providers"). Workiva and its Cloud Hosting Providers may record and collect aggregated and statistical data derived from the operation of the Services, including, without limitation, information related to Customer's subscription account activity (e.g., typical web analytics, which includes latency, packet size, hops, and source destination) (the "Aggregated Statistical Information"). Without limiting the confidentiality rights and protections set forth in this Agreement, Workiva owns the Aggregated Statistical Information. Nothing herein shall be construed as prohibiting Workiva from utilizing the Aggregated Statistical Information for purposes of operating Workiva's business, provided that Workiva's use of Aggregated Statistical Information will not reveal the following to any third party, whether directly or indirectly: (a) the identity of Customer or its Users, and/or (b) any Customer Confidential Information of Customer.

3.0 Fees; Payment.

3.1 Invoicing. Fees for Services ("Fees") will be set forth in each applicable Order and Customer shall pay such Fees in advance and/or in accordance with any billing frequency or terms stated in the applicable Order. Unless otherwise specified in the applicable Order Customer shall pay all undisputed Fees no later than thirty (30) days from receipt of invoice. If Customer has not paid all undisputed Fees in full within forty-five (45) days from receipt of invoice, Workiva has the right to suspend provision of Services until full payment is paid by Customer. If Customer disputes any Fees invoiced, Customer may provide Workiva written notice of such dispute within fifteen (15) days from receipt of the applicable invoice; failure to do so will forfeit Customer's right to withhold payment. Customer and Workiva will then work in good faith to attempt to resolve such contested amounts, provided, however, that Customer will remain responsible for the portion of Fees that are not disputed.

3.2 Subscription Fees. Fees for Subscription Services will be pursuant to the metric expressly agreed upon in a Subscription Order if applicable (e.g., number of users, annual revenue). To the extent Customer exceeds such metric, Workiva may charge Customer additional Fees which will be calculated based upon the pricing set forth in the applicable Subscription Order on a pro-rata basis based on first day of the calendar month in which such metric was exceeded. Upon Workiva's request, Customer shall execute documentation memorializing the change to the scope of its fees whether based on number of Users or other metric. In the absence of a new Order, Customer will remain responsible for associated Fees for future Subscription Terms.

3.3 Taxes. Fees stated in the Orders do not include applicable taxes. Except for taxes based on Workiva's net income or property, Customer shall be responsible for

payment of all applicable taxes, impositions, fees, or other charges that arise in any jurisdiction as a result of the Services provided under the Agreement, including without limitation all sales, use, value added, consumption, gross receipts (other than in lieu of net income tax), excise, stamp or transfer taxes, however designated. Customer shall pay any such tax when due or reimburse Workiva as Workiva may request. If Customer is exempt from such taxes, Customer shall provide Workiva with a certificate or permit documenting this exemption. If Customer is required to withhold or deduct any portion of the Fees, then Workiva shall be entitled to receive from Customer such amounts as will ensure that the net receipt, after tax and duties, to Workiva in respect of the Fees is the same as it would have been were the payment not subject to the tax or duties. If Workiva is required to pay any taxes on behalf of Customer due to a change in facts, circumstances, or tax legislation, the full amount of such tax will be billed to Customer separately, whether or not during the Agreement Term and promptly paid by Customer as further limited by any applicable statute of limitations. Workiva and Customer agree to cooperate to reduce any tax liability related to this Agreement.

3.4 Purchase Orders; Payment Processors. To the extent Customer requires the use of a purchase order prior to making any payments under the Agreement, Customer's failure to submit such purchase order to Workiva does not excuse Customer from payment of the Fees in the amounts, or in the manner, agreed upon herein or in the applicable Order. For the avoidance of doubt, invoices and/or the Fees therein may not be disputed for Customer's failure to provide administrative information, including purchase order numbers, contract numbers or IDs, or any other administrative information of a similar or related nature. If Customer requires the use of a third party for invoice processing, Customer shall be the sole bearer of any cost and expense associated with such third party.

3.5 Fee Increases. Unless otherwise specified in an Order Workiva may increase Fees for the Subscription Services not more than once in each twelve (12) month period upon thirty (30) days prior written notice to Customer. Customer will only be responsible for increased Subscription Service Fees for those Subscription Terms subsequent to the Subscription Term in which Customer received such price increase notice. For the avoidance of doubt this Section 3.5 shall apply to recurring Fees for Professional Services set forth in an automatically renewing Order or that do not otherwise expire pursuant to the terms of an Order. In addition, once the parties have entered into a Service Order, Workiva may not increase such underlying Fees (absent an agreed upon amendment or Change Order), provided that, after completion of the agreed upon Professional Services Workiva may increase the Fees associated with its general Professional Service offerings in its sole discretion.

4.0 Term; Termination.

4.1 Agreement Term. The Agreement begins on the Start Date of the first Order between the parties hereto, and shall continue until all Orders associated with the

Agreement have expired or been terminated (the “Agreement Term”), subject to Section 10.11.

4.2 Subscription Term. Unless otherwise specified in a Subscription Order, the Subscription Services will: (a) begin on the start date in the applicable Subscription Order and remain in effect for the period specified therein (the “Subscription Term”), and (b) automatically renew for the same period of time as the initial Subscription Term until either party notifies the other in writing that it will not renew at least thirty (30) days prior to the expiration of the then current Subscription Term. Regardless of Customer’s notice of non-renewal, Customer will remain responsible for the Fees associated with the then current Subscription Term.

4.3 Service Order Terms. The period of performance set forth in Orders for Professional Services will be as agreed upon by the parties and set forth in the applicable Order.

4.4 Termination for Convenience. Customer may terminate the Agreement or an Order without cause upon thirty (30) days written notice. If Customer terminates without cause, Customer will not receive a refund for any prepaid Subscription Services Fees, but Workiva will refund any prepaid and unearned Fees for Professional Services outstanding as of the effective date of termination. Any unpaid Fees due shall be payable by Customer on or prior to the effective date of such termination. Workiva may terminate an Order without cause upon ninety (90) days written notice, provided that it shall refund all unearned Fees within thirty (30) days of the termination effective date.

4.5 Termination for Material Breach. Either party may terminate the Agreement, or any ¬individual Order, for a material breach by the other party that is not cured within thirty (30) days after written notice of such material breach. The non-breaching party may elect to terminate the applicable Order only or the Agreement as a whole (and thus, all Orders hereunder). In the event the Agreement is terminated due to Workiva’s uncured material breach, Workiva will refund all unearned Fees within thirty (30) days of the termination effective date.

4.6 Termination for Bankruptcy. Either party may terminate the Agreement or any Order, or suspend its performance hereunder or thereunder, if the other party becomes insolvent or bankrupt or ceases to do business.

4.7 Survival. Neither expiration nor termination of the Agreement will terminate those obligations and rights of the parties pursuant to provisions of the Agreement which by their express terms are intended to survive and such provisions will survive the expiration or termination of the Agreement. Without limiting the foregoing, the respective rights and obligations of the parties under Sections 4.7, 5, 6, 7, 9, and 10 of these Master Terms and Conditions will survive the expiration or termination of the Agreement regardless of when such termination becomes effective.

5.0 Confidentiality.

5.1 Confidential Information. In connection with the Agreement, each of the parties may disclose to the other party information that relates to the disclosing party's or disclosing party's customers' business operations, financial condition, customers, products, services, or technical knowledge ("Confidential Information"). Except as otherwise specifically agreed in writing, each party agrees that: (a) all information communicated to it by the other in connection with the Agreement and identified as confidential, (b) any information exchanged between the parties in connection with Customer's purchase of any additional Services, and (c) all information communicated to it that reasonably should have been understood by the receiving party, because of confidentiality, descriptions or similar legends, the circumstances of disclosure or the nature of the information itself, to be confidential to the disclosing party, will be Confidential Information and will be deemed to have been received in confidence and will be used only for purposes of the Agreement. "Confidential Information" includes the information exchanged between the parties related to future business relationships or Services not currently addressed under the Agreement, including but not limited to requests for proposals, bids, correspondence, negotiations, and discussions. Any non-disclosure agreement entered into by the parties after the Effective Date shall be of no force or effect unless such non-disclosure agreement by its terms expressly supplements, modifies, or replaces this Section 5 of these Master Terms and Conditions. Workiva Confidential Information includes the Software, Services, Fees, the terms of the Agreement, development plans, and any security specifications, reports or assessments related to the Software, Workiva or its Cloud Hosting Providers. Customer Confidential Information includes Customer Data.

5.2 Standard of Care; Third Parties. Each party will use at least the same degree of care to safeguard and to prevent disclosing to third parties the Confidential Information of the other as it employs to avoid unauthorized disclosure or publication of its own information (or information of its customers) of a similar nature, and in any event, no less than reasonable care. Each party may disclose relevant aspects of the other party's Confidential Information to its employees to the extent such disclosure is reasonably necessary for the performance of its obligations, or the enforcement of its rights, under the Agreement; provided, however, that such party will use reasonable efforts to ensure that all such persons comply with these confidentiality provisions. Each party may disclose the other party's Confidential Information to third parties provided that such third parties are subject to (a) written confidentiality obligations at least as restrictive as those set forth in the Agreement, or (b) other professional or fiduciary obligations of confidentiality. These third parties are restricted to using the Confidential Information for the sole purpose of providing the contracted services to the party. Each party will be responsible for any improper disclosure of Confidential Information by such party's employees, agents, or contractors.

5.3 Preclusions on Use. Neither party will (a) use, or make any copies of, the Confidential Information of the other party except to fulfill its rights and obligations under

the Agreement, (b) acquire any right in or assert any lien against the Confidential Information of the other, or (c) sell, assign, lease, or otherwise commercially exploit the Confidential Information (or any derivative works thereof) of the other party. Neither party may withhold the Confidential Information of the other party or refuse for any reason (including due to the other party's actual or alleged breach of the Agreement) to promptly return to the other party its Confidential Information (including copies thereof) if requested to do so. Upon expiration or termination of the Agreement and completion of a party's obligations under the Agreement, each party will return or destroy, as the other party may direct, the other party's Confidential Information, and retain no copies. Workiva may fulfill the obligation to return Customer Data by providing one (1) User with access to the Software for a period not to exceed thirty (30) days solely to allow such User to obtain Customer Data. Subject to the foregoing confidentiality obligations, either party may retain copies of the Confidential Information of the other party to the extent required to document its performance or for compliance with applicable laws or regulations.

5.4 Exclusions; Permitted Use. This Section 5 will not apply to any particular information that either party can demonstrate (a) was, at the time of disclosure to it, in the public domain, (b) after disclosure to it, is published or otherwise becomes part of the public domain through no fault of the receiving party, (c) was in the possession of the receiving party at the time of disclosure to it and was not the subject of a pre-existing confidentiality obligation, (d) was received after disclosure to it from a third party who had a lawful right to disclose such information (without corresponding confidentiality obligations) to it, or (e) was independently developed by or for the receiving party without use of the Confidential Information of the disclosing party. In addition, a party will not be considered to have breached its obligations under this Section 5 for disclosing Confidential Information of the other party to the extent required to satisfy any legal requirement of a competent governmental or regulatory authority, provided that promptly upon receiving any such request, and to the extent it is legally permissible, such party advises the other party prior to making such disclosure and provides a reasonable opportunity to the other party to object to such disclosure, take action to ensure confidential treatment of the Confidential Information, or (subject to applicable law) take such other action as it considers appropriate to protect the Confidential Information.

5.5 Unauthorized Access. Each party will: (a) notify the other party promptly of any material unauthorized possession, use, disclosure, or knowledge of the other party's Confidential Information by any person that may become known to such party, (b) promptly furnish to the other party details of the unauthorized possession, use, disclosure, or knowledge, or attempt thereof, and use reasonable efforts to assist the other party in investigating or preventing the recurrence of any unauthorized possession, use, or knowledge, or attempt thereof, of Confidential Information, (c) use reasonable efforts to cooperate with the other party in any litigation and investigation against third parties deemed necessary by the other party to protect its proprietary rights, and (d) promptly use reasonable efforts to prevent a recurrence of any such unauthorized possession, use, or knowledge of Confidential Information.

5.6 Log-Ins and Passwords. In addition to the foregoing obligations, Customer agrees to hold the Software, Subscription Services and all associated log-ins and passwords in confidence, and to protect the confidential nature thereof, and shall not disclose any trade secrets contained, embodied, or utilized therein, to anyone other than a User having a need for such disclosure, and then only to allow use of the Software as authorized herein. Customer shall take all reasonable steps to ensure that the provisions of this Section 5.6 are not violated by any employee, User, or any other person under Customer's control or in its service.

6.0 Ownership; Usage Restrictions.

6.1 Workiva Ownership. Workiva (or its licensors, as the case may be) retains all ownership of and title to, and all intellectual property rights in, the Software, Services, and all software, equipment, processes, facilities, and materials utilized by or on behalf of Workiva to provide the same, including all patents, trademarks, copyrights, trade secrets, and other property or intellectual property rights. Customer acknowledges and agrees that Workiva (or its licensors, as the case may be) shall own all right, title and interest in and to any modifications, derivative works, changes, expansions or improvements to the Software, and Services, without any other or subordinate right whatsoever being held by Customer. Customer shall acquire no rights therein other than those limited rights of use specifically conferred by the Agreement. Customer may not create derivative works based upon the Software, or Services in whole or in part, or develop or request third parties to develop or modify any software based on ideas, processes, or materials incorporated therein. Customer shall not delete, remove, modify, obscure, fail to reproduce, or in any way interfere with any proprietary, trade secret, or copyright notice appearing on or incorporated in the Software. All rights related to the Software, or Services that are not expressly granted to Customer under the Agreement are reserved by Workiva (or its licensors, as the case may be). In the event that Customer provides Workiva with any comments, suggestions, or other feedback with respect to the Software, or Services, Customer hereby grants Workiva a perpetual, irrevocable, royalty-free, fully paid-up, worldwide license to use any such feedback, and Workiva has the right, but not the obligation, to use such feedback in any way without restriction or obligation to Customer. Workiva will be the exclusive owner of, and will be free to use for any purpose, any ideas, concepts, know-how, or techniques that result from Customer or Users' feedback, including, without limitation, any modifications or enhancements to the Software, or Services. Upon Workiva's reasonable request, Customer agrees to execute such additional documents if necessary for perfecting or recording Workiva's ownership interest, provided that preparation of such additional documents shall be at the expense of Workiva.

6.2 Customer Ownership. As between Workiva and Customer, Customer is, and will remain, the owner of all Customer Data. With the exception of a limited license granted to Workiva to use Customer Data solely for the purpose of performing the Services, Workiva acquires no right, title, or interest from Customer or its Users to

Customer Data, including any intellectual property rights therein. Any reports or documents generated through Customer's use of the Software in accordance to this Agreement will be owned by Customer. If such reports or documents include any pre-existing intellectual property owned by Workiva, Workiva hereby grants to Customer a perpetual, nonexclusive, royalty-free license to copy, modify, create derivative works of and distribute, license and sublicense such pre-existing intellectual property to the extent made a part of Customer's reports or documents.

6.3 Software Usage Restrictions. Customer and its Users may access and use the Software (a) for Customer's business use only, (b) solely as set forth, and subject to any restrictions, in the Agreement, and (c) not for the benefit of, or to provide services to, any third party. Customer shall not grant rights of access to the Software to anyone other than Users without Workiva's prior written consent. The rights granted to Customer under the Agreement may not be sold, resold, assigned (except as set forth in Sections 1 and 10), leased, rented, sublicensed, or otherwise transferred or made available for use by third parties, in whole or in part, by Customer without Workiva's prior written consent. For the avoidance of doubt, Customer may allow an Affiliate to use the Software under Customer's Order for such Affiliate's benefit, subject to Section 1. Customer shall not employ any techniques or make use of any services, automated or otherwise, designed to represent Users of the Software, or to represent, or misrepresent, Customer's Users' activity, including without limitation by the use of bots, botnets, screen scrapers, scripts, apps, plugins, extensions or other automated means to register accounts, log in, add new Users, send messages, post comments, or otherwise to act on Customer's behalf. Customer shall not gain or attempt to gain unauthorized access to any portion of the Software (including any application programming interfaces in the Software), or its related systems or networks, for use in a manner that would exceed the scope granted under the Agreement, or facilitate any such unauthorized access for any third party. If any unauthorized access occurs, Customer shall promptly notify Workiva of the incident and shall reasonably cooperate in resolving the issue. Customer shall not reverse engineer, decompile, or disassemble any Software or otherwise attempt to discover the source code thereof or permit any third party to do so. Customer shall not attempt to disable or circumvent any security measures in place. Customer may not knowingly reproduce or copy the Software, in whole or in part. Customer shall not modify, adapt, or create derivative works of the Software. Customer shall not use the Software to store or transmit libelous or otherwise unlawful or tortious material or any material in violation of third party privacy rights. Customer shall not knowingly interfere with or disrupt the integrity or performance of the Software or third party data contained therein.

7.0 Warranties; Disclaimers.

7.1 Mutual Representations and Warranties. Each party represents and warrants to the other party that: (a) it is duly organized, validly existing, and in good standing as a corporation or other entity under the laws of the jurisdiction of its incorporation or other organization, (b) it has, and throughout the Agreement Term, will retain, the full right,

power, and authority to enter into the Agreement and perform its obligations hereunder, (c) the execution of any of the documents that comprise the Agreement by its representative has been duly authorized by all necessary corporate or organizational action of such party, and (d) when executed and delivered by both parties, an Order incorporating these Master Terms and Conditions will constitute the legal, valid, and binding obligation of such party, enforceable against such party in accordance with its terms.

7.2 Workiva Representations and Warranties. Workiva warrants (a) that the Software will perform materially in accordance with the Documentation and the Agreement, (b) to use best efforts to correct material defects that are reported by Customer or its Users and otherwise provide the Subscriptions Services as further set forth in the Service Levels (if a malfunction is due to a problem with Customer hardware or software, Workiva will so inform Customer and it will be Customer's responsibility to obtain and pay for any repairs or modifications required for such Customer hardware or software), (c) the Services will be performed in a timely, professional, and workmanlike manner with a level of care, skill, practice, and judgment consistent with commercially reasonable industry standards and practices for similar services, using personnel with the requisite skill, experience, and qualifications, and will devote adequate resources to meet Workiva's obligations under the Agreement, (d) the Documentation will be reasonably updated so that it continues to describe the Software and Services in all material respects, and (e) to the best of its knowledge, the Software does not contain code whose purpose is to disrupt, damage, or interfere with Customer systems, software, or Customer Data.

7.3 Customer Acknowledgements. Customer accepts responsibility for selection of the Services to achieve Customer's intended results. Customer is solely responsible for obtaining all necessary rights and consents to enter Customer Data into the Software and hereby warrants that providing Customer Data to Workiva under the Agreement will not violate or infringe the rights of any third party. Customer further acknowledges that neither Workiva nor the Software is a primary system of record of Customer Data, and Customer shall regularly backup any files for which it intends as such.

7.4 Disclaimers. EXCEPT AS SPECIFICALLY SET FORTH IN THE AGREEMENT, TO THE FULLEST EXTENT PERMITTED BY LAW, THE SOFTWARE AND SERVICES ARE PROVIDED "AS IS." WORKIVA, ITS LICENSORS, AND SERVICE PROVIDERS DO NOT MAKE ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING THE WARRANTIES OF DESIGN, MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR ARISING FROM A COURSE OF DEALING OR USAGE OF TRADE, AND WORKIVA EXPRESSLY DISCLAIMS ANY AND ALL SUCH WARRANTIES TO THE FULLEST EXTENT PERMITTED BY LAW. Workiva does not warrant that the Software or Subscription Services: (a) will be uninterrupted or error free or (b) will operate in combination with other hardware or software unless such hardware or software is Third Party Software or hardware or software expressly approved or recommended by Workiva. Customer acknowledges and agrees that Workiva and its

licensors are not responsible for: (i) the accuracy or integrity of any Customer Data, (ii) the performance of Customer's or its Users' equipment, (iii) delivery of services or connectivity provided by third parties to Customer and its Users, or (iv) any loss or corruption of Customer Data that occurs as a result of transmitting or receiving Customer Data or viruses due to Customer's, or its Users', connection and access to the internet.

8.0 Infringement Indemnification.

8.1 Obligation to Defend. Workiva will (a) defend Customer from and against any claim by a third party alleging that the Software, when used as authorized under the Agreement, directly infringes such third party's patents, copyrights, or trademarks, and (b) in relation to such claim, indemnify and hold harmless Customer from any damages and costs finally awarded or agreed to in settlement by Workiva (including reasonable attorneys' fees).

8.2 Notice of Obligation. Workiva's obligations under Section 8.1 are expressly conditioned on the following: Customer shall (a) promptly notify Workiva in writing of any such claim of which Customer has actual knowledge (provided that failure to do so will only release Workiva from this obligation to the extent that such failure led to material prejudice), (b) in writing, grant Workiva sole control of the defense of any such claim and of all negotiations for its settlement or compromise, provided that no such settlement or compromise may impose any monetary or other obligations on Customer, and (c) reasonably cooperate with Workiva to facilitate the settlement or defense of the claim.

8.3 Replacement Software. Should the Software become, or of in Workiva's opinion is likely to become, the subject of a claim of infringement of a patent, trade secret, trademark, or copyright, Workiva may (a) procure for Customer, at no additional cost to Customer, the right to continue to use the Software, (b) replace or modify the Software, at no cost to Customer, to make it non-infringing, provided that the same function is performed by the replacement or modified Software, or (c) if in Workiva's judgment the right to continue to use the Software cannot be reasonably procured or the Software cannot reasonably be replaced or modified, terminate the Agreement (or the applicable Order) and grant Customer a pro-rated refund of any advance Fees paid applicable to the remainder of the Subscription Term.

8.4 Limitation. This Section 8 states the entire liability of Workiva with respect to infringement arising from Workiva software, or any parts thereof, and Workiva shall have no additional liability with respect to any alleged or proven infringement.

9.0 Limitation of Liability.

9.1 SUBJECT TO SECTION 9.2 AND TO THE FULLEST EXTENT PERMITTED BY LAW, (A) IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER FOR

SPECIAL, INDIRECT, INCIDENTAL, CONSEQUENTIAL, PUNITIVE, OR EXEMPLARY DAMAGES IN CONNECTION WITH THE SOFTWARE, SOLUTION, SERVICES, OR THE PERFORMANCE OR NONPERFORMANCE OF SERVICES OR ANY ORDER, REGARDLESS OF THE THEORY OF LIABILITY, EVEN IF SUCH PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, (B) IN NO EVENT WILL EITHER PARTY BE LIABLE TO THE OTHER PARTY FOR ANY LOSS OF REVENUES, LOSS OF PROFITS, LOSS OF BUSINESS, OR LOSS OF DATA, ARISING OUT OF CUSTOMER'S FAILURE TO USE THE SOFTWARE IN ACCORDANCE WITH THE DOCUMENTATION, AND (C) ¬ WORKIVA'S MAXIMUM LIABILITY UNDER THE AGREEMENT IS LIMITED TO THE FEES PAID BY CUSTOMER (EXCLUDING APPLICABLE TAXES) UNDER THE APPLICABLE ORDER TO WHICH THE CLAIM RELATES DURING THE TWELVE (12) MONTHS PRECEDING THE DATE ON WHICH THE CLAIM FIRST ACCRUED.

9.2 NOTWITHSTANDING THE ABOVE LIMITATIONS, THERE WILL BE NO LIMIT TO WORKIVA'S LIABILITY ARISING OUT OF (A) DEATH OR PERSONAL INJURY CAUSED BY WORKIVA'S NEGLIGENCE, (B) FRAUD OR FRAUDULENT MISREPRESENTATION, OR (C) ANY LIABILITY WHICH CANNOT LEGALLY BE EXCLUDED OR LIMITED.

10.0 Miscellaneous.

10.1 Public Announcements. Customer grants Workiva the right to use Customer's name, logo, trademarks, quotes, and/or trade names in press releases, product brochures, sales presentations, financial reports, webinars, and on its websites indicating that Customer is a customer of Workiva. All other public statements or releases require the mutual consent of the parties.

10.2 Non-Solicitation. Each party recognizes that the other party's employees constitute valuable assets. Accordingly, neither party will, during the Agreement Term and for a period of one (1) year thereafter, directly solicit any of the other's employees for positions of employment or as consultants or independent contractors. Notwithstanding the foregoing, neither party is precluded from (a) hiring an employee of a party that independently approaches it, (b) indirectly soliciting the other party's employees through the use of a staffing agency, provided that the party has not provided the staffing agency with names or other information to facilitate the solicitation of the other party's employee or contractor, or (c) conducting general recruiting activities, such as participation in job fairs or publishing advertisement in publications or on websites for general circulation.

10.3 Relationship of the Parties. The parties agree they are independent parties. Neither party shall be considered to be a partner, joint venture, employer, or employee of the other under the Agreement. The Agreement creates no agency in either party, and neither party has any authority whatsoever to bind the other party in any transaction or make any representations on behalf of the other party.

10.4 Notice. Any notice or demand which is required to be given under the Agreement will be deemed to have been sufficiently given and received for all purposes when delivered by hand, confirmed electronic transmission, or nationally recognized overnight courier, or five (5) days after being sent by certified or registered mail, postage and charges prepaid, return receipt requested, to the address, facsimile number, or the e-mail address identified in the applicable Order, and to the attention of such other person(s) or officer(s) as either party may designate by written notice.

10.5 Governing Law; Jurisdiction. Without regard to its conflicts of laws principles, the laws of Delaware govern all matters arising under or relating to the Agreement. Any and all actions, suits, or judicial proceedings upon any claim arising from or relating to this Agreement shall be instituted and maintained in the State of Iowa. If it is judicially determined that either party may file an action, suit, or judicial proceeding in federal court, such action, suit, or judicial proceeding shall be in the Federal District Court for the Southern District of Iowa.

10.6 Assignment. Neither party may assign the Agreement, or any of its interest herein, without the prior written consent of the other party, which consent may not be unreasonably withheld or delayed; provided, however, that no such prior approval shall be required for an assignment in connection with (a) a sale of all or substantially all of a party's business related to the subject matter of the Agreement, (b) any merger, sale of a controlling interest, or other change of control of such party, or (c) Workiva's assignment of all or part of its obligations under this Agreement to an Affiliate. In the event of assignment as mentioned in the previous sentence, the assigning party shall provide written notice as soon as is reasonably practicable. The Agreement applies to and binds the permitted successors and assigns of the parties.

10.7 Force Majeure. Neither party will be in default or otherwise liable for any delay in or failure of its performance under the Agreement if such delay or failure arises by any reason beyond its reasonable control, including any act of God or the common enemy or earthquakes, floods, fires, epidemics, riots, or failures or delays in transportation or communications (each, a "Force Majeure Event"). The parties will promptly inform and consult with each other as to any of the above causes which in their judgment may or could be the cause of a delay in the performance of the Agreement.

10.8 Injunctive Relief. Each party acknowledges and agrees that a breach, including an anticipatory or threatened breach, by either party of any of its obligations under Sections 5 or 6 may cause immediate and irreparable harm to the non-breaching party for which monetary damages may not constitute an adequate remedy. Accordingly, the breaching party acknowledges and agrees that the non-breaching party shall be entitled to seek injunctive relief for the breaching party's obligations herein, without the non-breaching party having to prove actual damages and without the posting of bond or other security. Such remedy shall not be deemed to be the exclusive remedy for the

breaching party's breach of the Agreement, but shall be in addition to all other remedies available to the non-breaching party at law or in equity.

10.9 Federal Government End Use Provisions. Workiva provides the Services and Software, including related software and technology, for ultimate federal government end use solely in accordance with the following: Government technical data and software rights related to the Software include only those rights customarily provided to the public as defined in these Master Terms and Conditions. This customary commercial license is provided in accordance with FAR 12.211 (Technical Data) and FAR 12.212 (Software) and, for Department of Defense transactions, DFAR 252.227-7015 (Technical Data-Commercial Items) and DFAR 227.7202-03 (Rights in Commercial Computer Software or Computer Software Documentation). If any portion of the Software is deemed "non-commercial," the Services are licensed under the terms hereof and under the RESTRICTED RIGHTS set forth in the applicable FARs and DFARs (and the government's use, duplication and disclosure rights are restricted as set forth therein). If a government agency has a need for rights not conveyed under these terms, it must negotiate with Workiva to determine if there are acceptable terms for transferring such rights, and a mutually acceptable written addendum specifically conveying such rights must be included in any applicable contract or agreement.

10.10 Pre-Release Data. The Parties acknowledge that Customer Data may include Customer material non-public information (the "Pre-Release Data") and that various laws may impose certain restrictions on trading securities of an issuer when in possession of Pre-Release Data and on communicating such information to any other person under circumstances in which it is reasonably foreseeable that such person is likely to trade in such securities based on such Pre-Release Data. Workiva confirms that its employees and service providers that have unencrypted access have been informed as to the confidential nature of Customer's Pre-Release Data and the importance of preserving its confidentiality, including refraining from trading in Customer's securities while in possession thereof.

10.11 Third Parties. Workiva Inc., its Affiliates and licensors, as well as Customer's Affiliates that receive access as set forth in Section 1, may be third party beneficiaries of the Agreement. No other third party, including without limitation Customer's addition of third party Users, is intended to be a beneficiary of the Agreement entitled to enforce its terms directly. As of the start date in Customer's initial Subscription Order unless otherwise stated therein there are no terms and conditions for Third Party Software with which Customer must comply. If after Workiva commences its provision of Subscription Services any underlying Third Party Software becomes subject to additional terms and conditions, upon reasonable prior written notice to Customer such terms may be attached to the Agreement, or otherwise incorporated by reference. If Customer does not consent to such terms it must notify Workiva of its rejection within thirty (30) days of receipt of such notice and, notwithstanding anything to the contrary in Section 4.1 of these Master Terms and Conditions, the Agreement will continue under the terms and conditions previously in place until the completion of all then active Subscription Terms,

at which time the Agreement and all Orders hereto will expire and be of no further force or effect. Workiva may subcontract provision of Services to its Affiliates and to third parties provided that it will remain responsible for breaches of the Agreement caused by such third parties.

10.12 Electronic Storage. The parties intend to allow for the electronic imaging and storage of the Agreement, and the admissibility into evidence of such an image in lieu of the original paper version of the Agreement. The parties stipulate that any computer printout of any such image of the Agreement shall be considered to be an "original" under the applicable court or arbitral rules of evidence when maintained in the normal course of business and shall be admissible as between the parties to the same extent and under the same conditions as other business records maintained in paper or hard copy form. The parties agree not to contest, in any proceeding involving the parties in any judicial or other forum, the admissibility, validity, or enforceability of any image of the Agreement because of the fact that such image was stored or handled in electronic form.

10.13 General. On the Effective Date, the Agreement supersedes all previous discussions, negotiations, understandings, and agreements between the parties with respect to its subject matter, including any non-disclosure agreements and/or obligations which will be expressly superseded in their entirety by Section 5 of these Master Terms and Conditions, and constitutes the entire Agreement between the parties. The parties shall reasonably cooperate with each other to provide such further assurances as may be reasonably required to better evidence and reflect, or to show the ability to carry out the intent, purposes, and obligations of the Agreement. No oral statements or material not specifically incorporated herein will be of any force and effect. With the exception of (a) modifications to the Documentation (which may not be unilaterally modified by Workiva except to ensure compliance with Section 7.2), (b) other URLs referenced in these Master Terms and Conditions or an Order (which may not be unilaterally modified by Workiva in a manner that would be detrimental to Customer in Customer's reasonable discretion), and (c) any terms or conditions associated with additional Services available for purchase via Workiva's website that have been accepted or acknowledged (electronically or otherwise) by Customer or a User, no changes in or additions to these Master Terms and Conditions will be recognized unless incorporated herein by amendment and signed by duly authorized representatives of both parties. With the exception of the Documentation, in the event Workiva updates a URL in accordance with the foregoing, and Customer determines such modification is detrimental to Customer, it shall so inform Workiva and Workiva will remain bound by the URL(s) previously agreed upon. For the avoidance of doubt, factual updates to the Documentation may not be voided by Customer in accordance with the foregoing. The application of Customer's general terms and conditions in any general vendor acknowledgement or Customer's other general purchasing conditions are hereby expressly excluded and objected to by Workiva. These Master Terms and Conditions shall apply and supersede the pre-printed terms and conditions of any form submitted, in electronic format or otherwise, by either party. The Agreement will not be

construed against either party as the purported drafter. The waiver by either party of a breach or violation of any provision of the Agreement shall be in writing, and (unless otherwise agreed in writing) will not operate as, or be construed to be, a waiver of any subsequent breach of the same or any other provision hereof. In the event any provision of the Agreement is held to be unenforceable for any reason, the unenforceability thereof will not affect the remainder of the Agreement, which will remain in full force and effect and enforceable in accordance with its terms. With respect to any unenforceable provision, the applicable arbitrator or court shall deem the provision modified to the extent necessary, in such adjudicator's opinion, to render such term or provision enforceable, and the rights and obligations of the parties will be construed and enforced accordingly, preserving to the fullest permissible extent the intent and agreements of the parties set forth herein. Headings in these Master Terms and Conditions shall not be used to interpret or construe its provisions. The following order of precedence will be followed in resolving any inconsistencies between the terms of these Master Terms and Conditions and the terms of any Orders, exhibits, statements of work, or other documents: first, the Sections 1 - 10 of these Master Terms and Conditions, including any referenced URLs (which may give priority to Orders for certain purposes); second, terms contained in an Order; and third, the terms of any other documents referenced in any of the foregoing.

USVN08122019

West Virginia Department of Administration Finance Division

Comprehensive Annual Financial Report Preparation Software/System
CRFQ 0209 FAR2000000002

Presented by:

Vertosoft LLC
1602 Village Market Blvd. #215
Leesburg, VA 20175

[redacted]
Certified Small Business Concern
Federal Tax ID: 81-3911287

Chet Hayes
Chief Technology Officer
571.707.4137
chet@vertosoft.com

www.vertosoft.com

2/14/2020

Table of Contents

1 Cover Letter 1
2 Company Description 3
3 Qualifications 13
4 Mandatory Requirements 14
5 Implementation 23
6 Pricing Page 25
7 Contract Manager 26
8 Attachments 27

1 Cover Letter

February 14, 2020

Melissa Pettrey
Senior Buyer
2019 Washington Street, East
Charleston, WV 25305

Dear Melissa,

Vertosoft, as the Authorized Government Reseller for Workiva, is pleased to respond to West Virginia Department of Administration Finance Division's request for quote for Financial Report Preparation Software/System. Herein you find a customized response detailing how our award-winning, FedRAMP authorized software, and experienced staff meet and exceed the requirements sought by the State.

Over 3,500 customers, including federal, state, city, county, special district, and corporate customers partner with Workiva as a low-risk solution to improve efficiencies within their organizations, modernize financial reporting, and streamline internal control management. Workiva understands the demands on government agencies and is committed to delivering solutions that support agencies' missions and employees.

Vertosoft recommends West Virginia Department of Administration Finance Division uses Workiva's connected financial reporting platform, called Wdesk, to produce the Comprehensive Annual Financial Report (CAFR). The Wdesk platform is a secure and integrated cloud-based tool that streamlines financial reporting. In addition, the Wdesk platform allows the State to achieve the following positive business outcomes:

- Eliminate version control issues using one collaborative tool with granular permissions;
- Ensure data accuracy and consistency using a single source of truth and linking capabilities;
- Improve coordination and communication between team members and reviewers using direct commenting and tasking;
- Provide complete accountability and transparency with a full audit trail.

Vertosoft's proposal represents a commitment to deliver the recommended solutions according to State's timeline, utilizing a Customer Success Manager and Solutions Architect. Should you have questions regarding the RFQ response, please contact me directly at 571.707.4137 or via email at chet@vertosoft.com. I look forward to discussing how the Wdesk platform supports the West Virginia Department of Administration Finance Division's mission and goals.

Respectfully,

Chet Hayes
Vertosoft
Chief Technology Officer

2 Company Description

About Workiva
Workiva (NYSE: WK) is the global leader in cloud-based connected reporting and compliance solutions. Founded in 2008 by software and business veterans, and incorporated December 10, 2014, Workiva's mission is to build trust in the global economy with transparent data and connected reporting. Workiva partners with organizations to transform how teams collaborate to manage and report with accuracy and accountability.

Workiva believes a collaborative, connected, consistent and continuous reporting and compliance platform addresses the lack of data assurance in today's complex business environment. Workiva builds engaging and intuitive business solutions that allow teams to maintain data integrity across all reporting and compliance processes, ensuring trust and reducing risk.

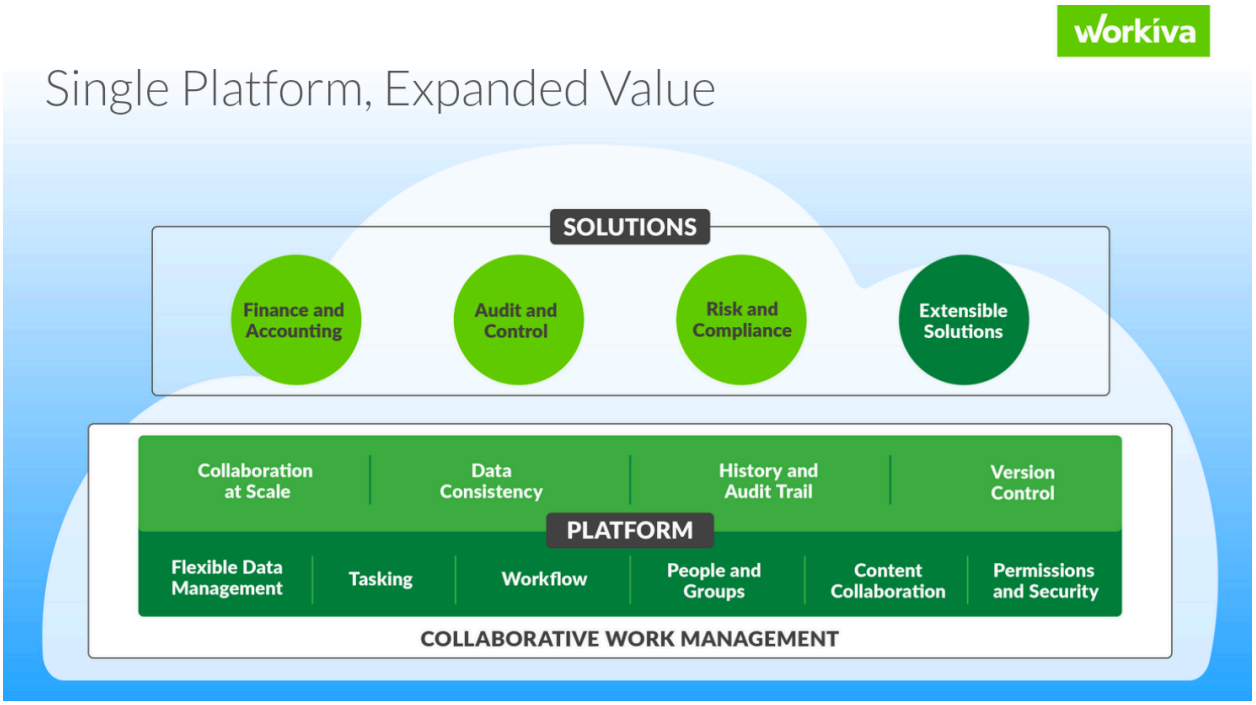
Today Workiva helps over 3,500 customers in 180 countries, including more than 75 percent of Fortune 500® companies, and over 200 government and higher education institutions, modernize their reporting and compliance processes with a connected platform. Our customers have created over 15 million reports, and linked over 5 billion data elements using the Wdesk platform.

Location
Workiva employs approximately 1,600 employees who are committed to understanding the customer's needs and care about the customer's success. Workiva's corporate headquarters is located at 2900 University Blvd, Ames, Iowa.

Additional US branch offices are in Boulder, CO, Bozeman, MT, Charleston, SC, Chicago, IL, Columbus, OH, Dallas, TX, Denver, CO, Missoula, MT, New York, NY, Philadelphia, PA, Scottsdale, AZ and Seattle, WA. Additional international branch offices are in Amsterdam, Frankfurt, Hong Kong, London, U.K., The Netherlands, Paris, Saskatoon, Sault Ste. Marie, Singapore and Sydney.

Wdesk Platform
The Wdesk platform connects people, processes and data in a single cloud-based tool. Wdesk supports controlled collaboration, version control, and data management for teams using business data from multiple sources and systems to achieve numerous goals. In addition, the platform includes a centralized repository of data that enables users to connect, access and analyze data from various sources called Wdata.

The familiar and intuitive design of Wdesk simplifies training and accelerates implementation. In addition, the platform removes the burdens of traditional software solutions, like costly and disruptive upgrades, and delivers application enhancements and optimizations seamlessly throughout the year.



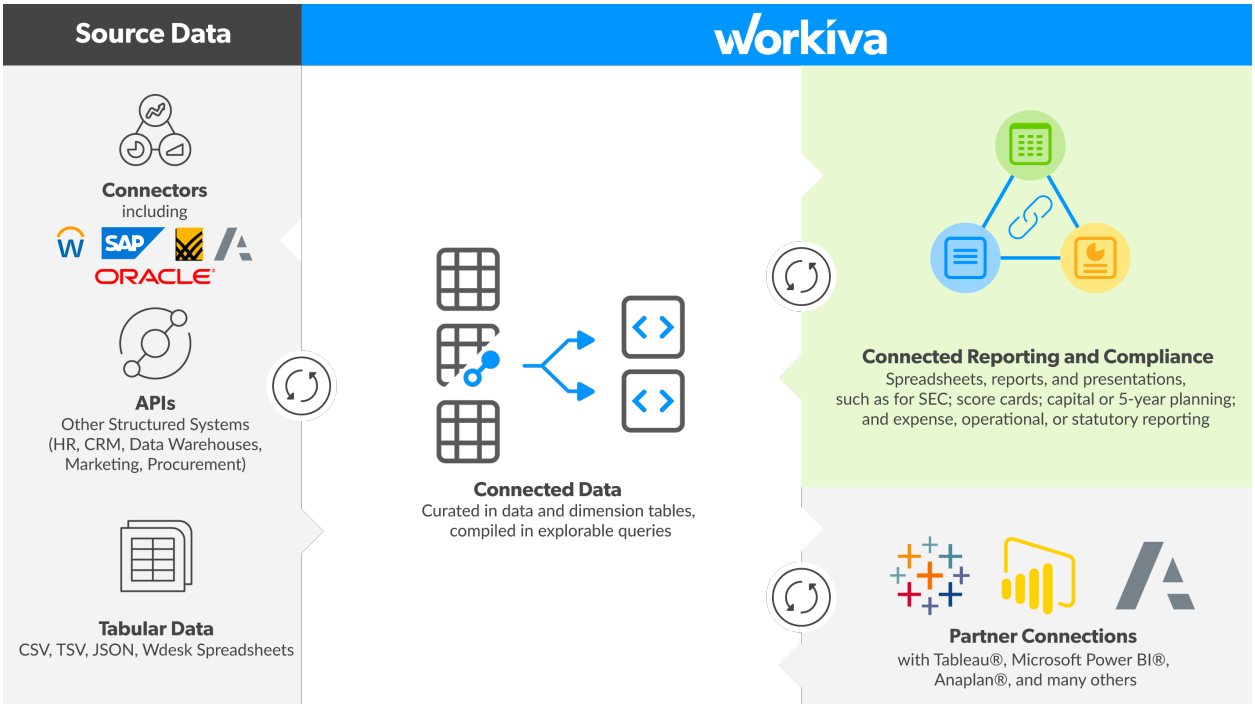
Data Consistency
Wdesk incorporates information from other source systems or files creating a single source of truth. Live-linked data is consistent and current, and available for numerous reporting and compliance needs.

Easy and Efficient
The familiar design makes setup easy and user adoption quick. Users understand the platform in less than two hours and can work from anywhere.

History and Audit Trail
Wdesk ensures consistency and accuracy in all steps of the business process. Every change is recorded with a digital time stamp and user information. Reviewers and auditors utilize the powerful communication and audit history information within the application.

Version Control
Teams work on the same versions of documents and data in Wdesk, eliminating version control issues. Teams also streamline communication using commenting and tasking feature within the platform.

Wdata
Wdata transforms how teams gather and prepare massive datasets and connect that data to Wdesk. Wdata consolidates datasets using common functions and custom scripts. Users securely share prepared data for financial reporting, planning and analysis. Wdata supports automated and on-demand updates, refreshing linked data and maintaining a full audit trail within the Wdesk platform. The connected data warehouse leverages pre-built connectors, application programming interfaces (APIs), and tabular data to source large volumes of data from systems of record, operational systems and spreadsheets.



Government agencies regularly use the Wdesk platform for the Comprehensive Annual Financial Report (CAFR) and Budget Book to drive productivity and value for employees and constituents, however the platform's financial reporting and compliance capabilities are more extensive.

- *Finance and Accounting*, including:
  - SEC (including Section 16 and Forms 10-K, 10-Q, 8-K, N-4, N-6 and Form S-1 and related IPO readiness),
  - Canada's System for Electronic Document Analysis and Retrieval (SEDAR)
  - eXtensible Business Reporting Language (XBRL)
  - Inline XBRL
  - Investor Relations including earnings call scripts and press releases
  - Data collection for financial footnotes
  - Statutory reporting
  - AFR, CAFR, PAFR and budgeting for state and local governments
  - Congressional Budget Justification
  - Financial reporting and planning for universities
  - Global Reporting Initiative (GRI)
  - Investments Compliance
  - Integrated financial planning
- *Audit and Controls* including:
  - Sarbanes-Oxley (SOX) compliance and Internal Controls over Financial Reporting (ICFR)
  - Controls management
  - Model Audit Rule (MAR) compliance
    - SOX certifications

        - SOX risk assessments / RCSA (risk control self assessment)
        - SOX scoping and planning
        - Narratives and process flow chart creation / maintenance
        - Evidence / PBC management
        - Testing and electronic annotations
        - Issues management, tracking, and reporting
        - Dashboards
        - Management / Audit Committee Reports
    - OMB Circular A-123
    - Audit Liaison
    - Audit Planning and Management
        - Audit Risk Assessments
        - Audit Fieldwork
        - Audit Reports and Memos
- *Risk and Compliance Management*, including:
    - Enterprise Risk Management
        - Enterprise risk assessments
        - Risk and control mapping -- documenting coverage by pillar or category
        - Risk memos and risk appetite documentation / tracking
        - Management dashboards, KRI reporting, and risk heat maps
    - Board reporting and a wide range of regulatory reporting such as
        - Own Risk Solvency Assessment (ORSA)
        - Solvency II
        - Resolution and Recovery Plans (RRP)
        - Comprehensive Capital Analysis and Review (CCAR)
        - Dodd-Frank Stress Testing (DFAST)
- *Operations*, including:
    - Strategic business plans
    - Monthly management reports
    - Managing and tracking key performance indicators (KPIs)
    - Integrated planning
    - Environmental, Health and Safety (EHS) reporting
    - Data collection for domestic sales
    - Performance reporting
    - Employee benefit financial statements

How It Works

Wdesk users collect business data from a variety of sources, like spreadsheets and systems of record, then link the data to required documents, presentations and spreadsheets. The data linking and document changes are supported by a full audit trail providing transparency and accountability in a collaborative environment. Granular permissions allow the team lead to set appropriate document access and control for collaborators with varying responsibilities. Implementation is timely and does not require IT support, allowing a quick transition to an efficient and trusted tool.

Vision
Workiva's vision is to simplify essential business and compliance reporting. The Wdesk platform removes the manual, cumbersome process of creating business, financial and managerial reports and delivers accurate data.

Founding Principles
- Provide the highest standard in cloud-based collaboration solutions for business reporting and compliance.
- Be the leader in technology innovation with a focus on usability.
- Operate with complete integrity and data security.
- Strive for 100 percent customer satisfaction by understanding and solving our customer challenges.

Security
Securing electronic data is paramount to confidential financial and strategic business information. Workiva invests in technology, people, and process to ensure customer information is safe, secure and private. Our dedicated team of software and security professionals is responsible for building in security from the start, reviewing all design, software code, and completed products to ensure strict security and data privacy standards.

Workiva selects security partners carefully and utilize Google and Amazon to deliver the scalability and reliability our customers require.

To demonstrate our commitment to security, Workiva has successfully completed the rigorous Service Organization Controls (SOC) 1 Type II and (SOC) 2 Type II with Health Insurance Privacy and Portability Act (HIPPA). For privacy, Workiva is TRUSTe certified, and adheres to all rules and best practices for HIPPA and General Data Protection Regulation (GDPR) compliance. These audits and certifications establish that Workiva utilities uniform and reliable safeguards and operational controls as a host and processor of our customers' data.

Workiva has achieved an Agency Authorization to Operate (ATO) under the FedRAMP Moderate Baseline program for Cloud Service Providers (CSP). FedRAMP, the Federal Risk and Authorization Management Program, is a comprehensive security program for cloud-service providers (CSPs) like Workiva. FedRAMP accelerates the adoption of cloud services by increasing confidence, consistency, and automation of security practices and continuous monitoring.

World Class Customer Satisfaction
Workiva is committed to our customers' success and supporting them throughout the reporting process, and our Customer Success teams thrive on delivering exceptional service.

Our culture is based on an innate caring and understanding of the customers' needs. Our Customer Success Managers are embedded in the customers' teams as they work together through all the processes and controls necessary for high-quality business data management, reporting and decision-making.

Our customers love the personal attention to detail and how we respond to them around the clock. Our customer satisfaction scores are greater than 95 percent, and our revenue retention rates exceed 95 percent, confirming Workiva is a trusted partner.

Our Customers
Since 2010, Workiva has provided our solutions to more than 3,500 enterprise customers, including over 75% of the FORTUNE 500®. Our customers include many of the world's leading companies. Fortune 100s, high-tech innovators, manufacturers, banks, government agencies, airlines, energy companies—businesses from Home Depot to Skilled Healthcare Group and Hyatt Corporation to Kimball International trust Workiva for their reporting needs. Some of our public sector customers include General Service Administration, State of Arizona, City of El Paso, Middlesex County, and the State University System of Florida.

Our Commitment
Workiva is committed to improving and understanding our customers' compliance, data management, and financial reporting responsibilities. Workiva is proud to sponsor NASC (National Association of State Controllers), NASACT (National Association of State Auditors, Controllers, and Treasurers), GFOA (Government Finance Officer's Association), and to be a corporate member of AGA (Association of Government Accountants). These organizations provide government leaders with tools, education, and networking opportunities to learn and share best practices both nationally and regionally.

Workiva's Leadership Team
Our executive management team scaled software companies from start-ups to private and public global enterprises.

Martin J. Vanderploeg, Ph.D.,
Chief Executive Officer and President
Former Founder, COO, Engineering Animation, Inc.

Mitz Banarjee,
Executive Vice President of Global Operations
Former Director of Client Services at Yodle (acquired by Web.com in 2016)

Troy M. Calkins,
Executive Vice President, Chief Legal and Administrative Officer and Corporate Secretary
Former Partner at Drinker Biddle & Reath LLP

Julie Iskow,
Executive Vice President and Chief Operating Officer
Former Chief Technology Officer, Medidata Solutions

J. Stuart Miller,
Executive Vice President, Treasurer and Chief Financial Officer
Former Founder and Managing Director, Colonnade Advisors
Former Managing Director, JP Morgan & Co.

Scott Ryan,
Executive Vice President of Global Sales
Former Vice President of North America Cyber Security Sales for IBM

Jeffrey D. Trom, Ph.D.,
Executive Vice President and Chief Technology Officer
Former Founder, CTO, Engineering Animation, Inc.

Jill E. Klindt,
Senior Vice President, Chief Accounting Officer and Treasurer
Former Manager of Financial Analysis at Financial Intelligence, LLC.

Board of Directors
David S. Mulcahy
Workiva Chairman of the Board; director and chairman of the audit committee of American Equity Investment Life Holding Company (NYSE: AEL); director, American Equity Investment Life Insurance Company of New York; chairman, Monarch Materials Group, Inc., successor to Monarch Holdings, Inc.; former executive officer of Monarch Holdings, Inc.; president and chairman of the board of directors of MABSCO Capital, Inc.

Michael M. Crow, Ph.D.
President of Arizona State University and Professor of Science and Technology Policy at ASU; former director of Aquila, Inc. (NYSE: ILA); consultant for the Moscow School of Management; former consultant for the Malaysian Global Science and Innovation Advisory Council; former member of Workiva's advisory board; former advisor to the U.S. Departments of State, Commerce and Energy; fellow, National Academy of Public Administration; member, National Advisory Council on Innovation and Entrepreneurship and Council on Foreign Relations.

Robert H. Herz
Member of the board of directors of the Sustainability Accounting Standards Foundation; former member of the Workiva advisory board; former audit partner at PricewaterhouseCoopers; President of Robert H. Herz LLC; former Chairman of the Financial Accounting Standards Board; member of the board of directors of the Federal National Mortgage Association ("Fannie Mae") since 2011 and of Morgan Stanley (NYSE: MS) since 2012; executive-in-residence at the Columbia University Business School.

Eugene S. Katz
Retired partner and board member, PricewaterhouseCoopers; former member of the Workiva advisory board; director of audit committee of Asbury Automotive Group (NYSE:ABG) since 2007; audit committee chair at ABG since 2009; member of ABG compensation committee since 2011.

Suku Radia
Retired Chief Executive Officer and director, Bankers Trust Company; former Chief Financial Officer of Meredith Corporation (NYSE: MDP); former mergers and acquisitions partner with KPMG LLP; director of Nationwide Insurance Company.

Martin J. Vanderploeg, Ph.D.
Founder, Chief Executive Officer and President, Workiva; former Chief Operating Officer and Managing Director of Workiva LLC; former founder, Executive Vice President and Chief Technology Officer of EAI; former tenured professor of mechanical engineering at Iowa State University; former founder and director of the Iowa State University Visualization Laboratory.

Brigid A. Bonner
Chief Experience Officer of CaringBridge; Previously, she was Senior Vice President of Strategy and Planning for OptumHealth. Before that, she was Senior Vice President and Chief Information Officer at UnitedHealth Technologies, a shared services architecture and infrastructure organization of UnitedHealth Group. She has also served in various technology and operational leadership roles with Simon Delivers, Target Corporation and IBM.

Thought Leadership

Robert Childree, Senior Advisor, Former State Comptroller of Alabama
Mr. Childree has over forty years' experience in financial management and governmental accounting systems. He has specific expertise in the area of financial management systems for state governments including accounting, budgeting, procurement, payroll, personnel (HR), financial analysis and financial reporting. Mr. Childree developed and wrote fiscal and accounting policy for the State of Alabama. He has developed and taught financial management courses to the fiscal staff of the State of Alabama and has spoken frequently regarding governmental financial reporting to various organizations across the country.

John Radford, Senior Advisor, Former State Controller of Oregon
John has many years of governmental financial management experience starting his career for the city of Omaha, Nebraska before moving to Oregon in 1983 to begin work as chief budget officer in the Oregon Judicial Department. John was appointed State Controller in 1989 and has since served several leadership roles within the State. John is a lifetime member and past president of NASACT and NASC. He has also been very involved with other organizations such as GFOA, AGA, and IIA to name a few.

Bob Attmore, Senior Advisor, Former GASB Chairman
Bob is a highly regarded accountability executive with demonstrated leadership and management skills developed over four decades of progressively more responsible positions in professional service organizations. He is experienced at building a shared vision for excellence and motivating a highly trained group of professionals, technical and clerical employees to achieve desired results. Bob is focused on accomplishments with a positive attitude, strong work ethic and a reputation for integrity. He has held top leadership positions in several professional associations, and has been a frequent speaker at professional conferences.

Hank Steininger, CEO, H.J. Steininger PLLC
Mr. Steininger brings years of professional and government experience, and is the CEO of a public accounting and professional services firm based in Palm Beach, Florida. For Grant Thornton LLP, he held the positions of Managing Partner, Global Public Sector, U.S. Chief Operating Officer, and member of the Partnership Board. Clients served included technology, financial services, not-for-profit and government organizations. He is a former partner with Ernst & Young and senior executive with ICF International. He has served as Chairman of the Association of Government Accountants (AGA) Corporate Partners and the Technology Association of America. Hank is a CPA in Florida and Virginia, holds additional certifications, and is an active member of the AICPA and the Florida and Greater Washington Societies of CPA's.

Workiva Employees
Workiva's values and leadership principles are core to all company practices, including hiring and professional development. The Human Resource team actively recruits employees who care about delivering an exceptional customer experience, and who have multiple years of experience in accounting, finance and integrated risk. Workiva conducts background checks on all candidates offered a position to verify education, certifications and previous employment.

Workiva believes our employees are the company's greatest asset, and gives employees the resources needed to meet customers' goals. The company culture is collaborative. We encourage diverse thought and expect employees to hold themselves and each other accountable. Employees act with urgency, trust one another, embrace change, constantly communicate and create new solutions every day.

It's not uncommon for Workiva staff to hold certifications in accounting, finance, information technology and project management, like Certified Public Accountant (CPA) or Project Management Professional (PMP). In addition, Workiva employees have typically worked for large accounting, banking, consulting, financial, information technology or software firms, and have experience with business intelligence technologies, databases and data management platforms as well as accounting and finance business applications like Oracle, SAP or Workday to name a few.

Awards & Recognition
Workiva's goal is to develop, launch, and support technology for the specific and intricate world of business data that impacts all parts of a company or agency. We strive to exceed our customers' expectations and design our platform functionality around their direct feedback.

We are honored to be recognized by Gartner for a third year in a row as Magic Quadrant Leader for Financial Close, by Chartis RiskTech100 for outstanding Customer Satisfaction and by other organizations for best overall SaaS solution, the best employer, the best place to work and sustainability practices.


COMPUTERWORLD
2019
100
BEST PLACES
TO WORK in IT


GOLD
2019 STEVIE
WINNER
FOR
GREAT EMPLOYERS


APPEALIE
2019
AWARD WINNER


VALUE
2019
grc2c


FORTUNE
100
BEST
COMPANIES
TO WORK FOR
2019


GOLD
2019 STEVIE
WINNER
AMERICAN
BUSINESS AWARDS

3 Qualifications

3.1 The proposed software solution must have been used for a minimum of 15 CAFRs that had successful submissions to the GFOA award program.

Since 2015 Workiva has been under contract with over 15 state controller's offices who have successfully published GFOA award-winning CAFRs and other reports.

3.2 Company must have experience with the implementation of at least five (5) state CAFRS.

State of Alabama, Department of Finance
2018 CAFR

State of Florida - Department of Financial Services
2018 CAFR

State of Georgia
2019 CAFR

State of Utah
2019 CAFR

State of Washington, Office of Financial Management
2019 CAFR

4 Mandatory Requirements

4.1.1 This RFQ is a request for software and implementation services to produce the state's CAFR. The Finance Division requests qualified vendors to submit a bid for implementation and installation with maintenance, support, warranty and hosting of a cloud-based software-as-a-service.

Workiva offers a 100% cloud-based software-as-a-service (SaaS) solution in a secure and centralized platform call Wdesk. Wdesk is owned, delivered and manage by Workiva to maximize flexibility and scalability for the customer. There are no additional costs for ongoing configuration, maintenance or upgrades/updates. Platform upgrades/updates are released weekly with no downtime or disruption to the customer.

General Requirements

4.1.1.01 Ability to produce GAAP/Uniform Guidance compliant financial statements and reports.

The Wdesk platform produces GAAP/Uniform Guidance compliant financial statements and reports, like the CAFR. Refer to the Wdesk Platform section of the proposal to review the extensive list of GAAP compliant financial statements and reports Wdesk supports.

4.1.1.02 Publish all components of the CAFR/Single Audit/SWCAP (cover/divider pages, organizational charts, graph, text files, spreadsheets, and pdfs) from a single software solution to a portable document format (pdf). Previously issues CAFR/Single Audit/SWCAPs can be found at www.finance.wv.gov/fars.

The Wdesk platform is a single software solution that allows government agencies to publish all components of the CAFR, Single Audit and SWCAP in a portable document format (pdf). For example, an agency can create a pdf document of the entire CAFR or any combination of documents within the CAFR. In addition, the agency can create a Publish Ready PDF for traditional printing and apply features like:

- Hyperlink formatting;
- Table cell background shading;
- Leader dots in cells;
- Use CMYK colorspace;
- Make ADA compliant.

4.1.1.03 Produce all components (graphs, text files, and spreadsheets) of the CAFR/Single Audit/SWCAP using a single software solution.

Wdesk is a multi-business reporting platform in a single software solution. Government agencies easily and efficiently produce all components of the CAFR, Single Audit and SWCAP within the platform because Wdesk:

- Provides the flexibility for government employees to collaborate across multiple reports in a controlled environment;
- Makes data, documents, presentations and spreadsheets created for the CAFR, Single Audit or SWCAP readily available and accessible for other reports;
- Links information from a single source of truth ensuring data accuracy and consistency throughout all reports replying on the same information.

4.1.1.04 Ability to save and review multiple versions including the final CAFR.

The Wdesk platform makes saving and reviewing versions easy by:

- Automatically saving all changes and edits every sixty (60) seconds;
- Automatically creating and storing a new version every five (5) minutes during active use;
- Creating blacklines.

To compare versions, the user selects two (2) different versions of the document from the history panel, and clicks create a blackline. Then Wdesk automatically compares the two (2) versions and produces a PDF noting all changes.

4.1.1.05 Provide designate support staff to address issues or technical problems and be based in the continental United States.

Workiva's solution-based licensing (SBL) includes Premium Support based in the continental United States, a dedicated Customer Success Manager (CSM), and access to a variety of training materials and resources at no additional cost.

The dedicated CSM is a trained application expert who directs day-to-day support activity for the customer, and communicates with Software Support, Product Development and other Workiva teams to ensure timely responses to customer questions, requests and incidents. The CSM is Wdesk certified and has experience working with government agencies on a variety of solutions.

Customer success is one of Workiva's core values. Employees thrive on delivering exceptional service, and our customer satisfaction scores and revenue retention rates exceed 95 percent.

Premium Support Includes:
Guaranteed two (2) hour response time
Basic support hours
24x7x365 on-call support
Dedicated Customer Success Manager (CSM)
Dedicated Initial and Ongoing Training
Online Help and Workiva User Community Access
Product Updates
Quality Success Reviews (QSR) with your Workiva team
Emergency Filing Services

24/7 Hotline Support (staffed by Workiva experts)*
*After basic account management support hours, customers will reach someone other than their dedicated Customer Success Manager for no additional fee.

Basic support hours are from 9 am to 5 pm, Monday through Friday based on the time zone of the nearest Workiva support center. Support center locations are in Eastern (ET), Central (CT), Mountain (MT) and Pacific (PT) Time Zones.

The 24x7x365 on-call customer success support includes a two (2)-hour maximum response time. The on-call customer success team includes members of the account management and technical teams who are responsible for smooth operation of the software and hosting infrastructure.

4.1.1.06 Provide full first-year implementation for the project.

Workiva provides full implementation services and works side-by-side with customers to rapidly adopt the solution. Customers are trained and working on reports within hours. Implementation varies based on size and scope of the project, but the typical implementation timeline is thirty (30) to forty-five (45) days. The familiar and intuitive design of Wdesk, and a dedicated CSM ensures a smooth implementation. Teams are comfortable with Wdesk's functionality as implementation concludes, and assured they can contact their CSM for assistance.

Refer to section 5 Implementation for additional implementation information.

4.1.1.07 Licensing must accommodate a minimum of 20 concurrent users.

Workiva’s solution-based licensing (SBL) supports an unlimited number of users at no additional cost. The internal owner or account administrator sets up user access, grants temporary access and removes access as needed. The unlimited user feature allows teams to easily expand and scale as needed.

Specific Requirements

4.1.1.10 Software needs to have the ability to import and map data from the state’s financial accounting software and other databases into the financial reporting software solution.

Wdesk makes is easy to connect and update data from users critical systems, including desktop spreadsheets and documents, general ledgers, ERP, CRM and other source systems into the platform. Wdesk offers direct import and export capabilities, application program interfaces (API) and pre-built connectors.

Bidirectional data flows between connected systems, and linked data within Wdesk gives users confidence information is correct and consistent. Direct imports from source systems and automatic refreshing eliminates manual entry errors and ensures data is up-to-date.

Workiva delivers comprehensive standards-based web service APIs to support integration to and from the Wdesk platform. The connections are built and maintained by the customer's IT team.

4.1.1.11 Incorporate documents from Microsoft Office products including Excel, Word, PowerPoint, etc.

The Wdesk platform is fully compatible with Microsoft Office. Users easily import Excel, Word and PowerPoint files into Wdesk as well as export documents, spreadsheets and presentations from Wdesk into Excel, Word, PowerPoint and PDF formats.

4.1.1.12 Produce financial statements on an accrual basis of accounting through the importing of data and journal entries.

The Wdesk platform allows government agencies to produce financial statements on an accrual basis of accounting.

Refer to requirement 4.1.1.10 for additional information on importing data in Wdesk.

4.1.1.13 Link financial statements, MD&A, footnotes, and schedules to supporting documents.

Wdesk allows users to link supporting documents to financial statements, MD&A, footnotes and schedules using the Attachments feature.

4.1.1.14 Link financial statements to MD&A, footnotes, and schedules that dynamically update changes throughout the document.

Live-linking is a core feature of Wdesk to maintain data accuracy and integrity. The familiar copy-paste function is used to create source and destination links. A single source value or single source text can link to several locations or destinations within Wdesk. When a source value or source text is updated so are all destination links throughout documents, presentations and spreadsheets. Each use of data can be formatted to different number types and decimal places without affecting the source data. Links can be rolled forward to new reporting periods. Link properties provide a view of all the uses of a linked value, and link history provides change details of who made the change with a corresponding date and time stamp.

4.1.1.15 Capable of updating financial statements and notes for future GASBs.

Wdesk is capable of updating financial statements and notes for future GASBs using the linking feature.

Refer to requirements 4.1.1.13 and 4.1.1.14 for addition linking information.

4.1.1.16 Create journal entries and track adjustments for the CAFR that dynamically update data across the statements via the journal feature.

The Wdesk platform supports two (2) journal entry preparation methods: Wdata; Wdesk spreadsheets.

Wdata
Wdata automates journal entry preparation using a feature called Chains and updates to linked financial statements accordingly. Chains allow a user to create and manage a linear sequence of tasks, like journal entry preparation and refresh linked data accordingly. Chains run on-demand and according to defined conditions like a specific interval, specific date range, or a trigger event.

Wdesk Spreadsheets
An adjustment template in Wdesk spreadsheets supports journal entry preparation and reconciles governmental fund statements and governmentwide statements. The template links data used for adjustments from the workpapers, then links the information to reconciliation pages and face statements, and dynamically updates data across linked statements.

4.1.1.17 Provide real-time comments and notifications to users within the software solution.

Direct commenting and tasking with automatic email notification is available within the collaborative Wdesk platform. Users easily add comments and assign tasks with due dates. All comments and tasks are tracked.

Commenting
Wdesk provides a robust commenting feature for teams that includes direct commenting and threaded discussion. The direct commenting feature allows a user to specifically address another user using a @username within the comment field. Once the comment is posted, an automatic email notification is delivered to the noted user. Then the noted user clicks the embedded link to directly review and address the comment. Comments are maintained in a threaded discussion format with dates and times, and can be filtered by user, status and date.

Tasking
Wdesk provides an integrated tasking solution for users to create, assign and complete tasks within documents, presentations or spreadsheets. To create and assign a task the user adds a task, detailing title, due date, description, assignee(s) and location (i.e., specific section of document or entire document). Once the task is created, the assignee receives an automatic email notification alerting him/her of the task. Reminder emails are automatically sent on the due date and the day after the due date, and the assigner can send reminders at any time. In addition, the assigner can edit, view activity and mark tasks as completed all within the collaborative platform.

4.1.1.18 Allows the ability to sort comments by user, opened/closed, and time frame.

Wdesk allows users to sort comments by user, open/closed status, time frame (i.e., today, before MM/DD/YYYY, between) and content.

4.1.1.19 Software must have automatic save function every sixty (60) seconds.

Wdesk automatically saves content every sixty (60) seconds.

4.1.1.20 Provide for multiple users to access the software solution simultaneously without overriding or conflicting versions.

Controlled collaboration is a core feature of Wdesk. Multiple users work simultaneously on the same document with real-time updating, eliminating the need for numerous versions of documents, presentations and spreadsheets.

In addition, Wdesk includes an essential feature called Share that restricts multiple users from editing the same section at the same time. When a user is working on a specific section of a document, presentation or spreadsheet, that section changes to draft mode. In draft mode other users are restricted from making changes to that section until the user shares his/her changes. Restricted users can see who is making changes.

A new version of a document, presentation or spreadsheet is created each time a user shares changes. Historical versions of documents, presentations and spreadsheets are accessible to users via the History Panel with user, date and time information. Comparing historical versions is simple using blacklines.

Refer to requirement 4.1.1.04 and 4.1.1.26 for additional information on comparing historical versions.

4.1.1.21 Provide for only one user having access to change the documents at a time.

The Wdesk platform includes a feature called Share the restricts multiple users from editing the same section at the same time.

Refer to requirement 4.1.1.20 for additional information regarding the Share feature.

4.1.1.22 System capable of supporting future inline XBRL requirements.

Workiva is a world leader in XBRL technology and support services, and is capable of supporting inline XBRL requirements. Currently, more than 75% of Fortune 500® companies use the Wdesk platform to tag and summit to the SEC. In addition, two (2) dedicated full-time Workiva employees actively participate in the XBRL-US State and local working group. The working group successfully developed the first taxonomy for tagging CAFRs and submitting in electronic format.

Workiva is committed to supporting all future government wide XBRL/iXBRL mandates. In fact, one of Workiva's sales engineers, Cathlyn Coons, authored an article about the future of the modern CAFR and completed XBRL tagging for the states of Georgia and Utah as part of a pilot project. Access additional information at https://www.workiva.com/blog/leading-way-modern-cafr.

Internal Control Requirements

4.1.1.23 Provides a full audit trail of every change made to the report(s).

Wdesk provides a complete audit trail solution, logging all activity, changes, deletions, edits and updates by user with date and time stamp. Wdesk automatically saves every sixty (60) seconds, backing up all changes and edits, and a new version is created every five (5) minutes during active use. Users easily review historical versions of reports by creating blacklines.

Refer to requirement 4.1.1.04 for additional information on comparing historical versions.

4.1.1.24 Creates a record of all changes made to a file (database) and maintains an audit trail or log of all operations, including the import of every audit test, carried out on the database. Entries are tagged with the user id from login.

Wdesk creates a digital record of all changes to files and databases and makes the information available in the History Panel. The digital record includes user, date and time information. For example, changes are tracked at the cell level within a spreadsheet and a user can view who changed it, what changed and when it changed. The full audit trail makes it easier for teams to collaborate and provides accountability.

4.1.1.25 Compares, joins, appends, and connects different files from different sources.

The Wdesk platform allows users to compare, join, append and connect different files from different sources. For example, a team using multiple documents and spreadsheets to create the CAFR, can bring all those files into the collaborative and controlled Wdesk environment.

4.1.1.26 Allows users to compare two (2) versions of the report to visually identify which elements of the report have changed.

Wdesk supports version comparison by quickly creating blacklines in PDF format. The ability to only include pages with changes, and color-coded notations of additions in blue text and deletions in red strike-through text make it easy to review changes between revisions.

Refer to requirement 4.1.1.04 for additional information on comparing historical versions.

4.1.1.27 Provides user- and/or role-based security within a document or report.

Wdesk supports user- and role-based security. The internal administrator or account administrator sets different levels of permissions for users and roles, controlling all users' ability to modify and/or view content. Wdesk security permission are granular to achieve controlled collaboration and varied levels of control within a single document.

Additional Advanced Permissions controls include:

- Distribute role-based document access and privileges for administrators, contributors and reviewers;
- Set permissions at the cell, document or section level;
- Owner, editor, viewer, and no access permission levels;
- Approve and reject proposed changes permission levels.

4.1.1.28 Supports the review cycle where multiple participants can review and comment on the draft(s) of the report(s).

The Wdesk platform simplifies and streamlines the review process for multiple participants with controlled collaboration. Multiple participants review, make comments and assign tasks within the same document, presentation and spreadsheet eliminating version control issues. In addition, the collaborative environment allows teams and reviewers to communication within the application instead of communicating through individual or lengthy group emails.

Refer to requirement 4.1.1.17 for additional commenting and tasking information.

4.1.1.29 Provide Service Organization Controls (SOC) 1 and 2 Statements on Standards for Attestation Engagement No. 16 (SSAE 16).

Workiva produces yearly SOC Type 1 and SOC Type 2 reports. The current SOC 1 Type II Report and SOC 2 Type II Report are included as part of the submission. These reports are also available on Workiva's compliance portal for review: https://www.workiva.com/security/compliance-document-portal.

In addition, Workiva is FedRAMP authorized at the moderate security impact level for a broad range of connected reporting and compliance solutions available to all federal agencies.
FedRAMP Authority to Operate (ATO) Details
Authorization Date: 10/9/2019
Service Model: SasS
Impact Level: Moderate
Status: FedRAMP Authorized
[redacted]
Authorization Type: Agency
Independent Assessor: Coalfire System, Inc.
The Federal Risk and Management Program Dashboard

Formatting Requirements

4.1.1.30 Must produce highly formatted report output.

Wdesk combines word processing, linked workbooks, charts, graphs, tables and presentations in a single software solution that allows government agencies to create highly formatted report outputs. Adobe PDF, Microsoft Office and Indesign are report output options in Wdesk.

4.1.1.31 Allows for advanced formatting features within the application.

Wdesk includes advanced formatting features similar to Microsoft Office and Adobe Acrobat as well as Style Guides. A Style Guide is recommended when a document owner wants/needs to repeatedly apply the same formatting. The document owner creates and edits the Style Guide and makes it available to other users to ensure consistent formatting. Applying a style is as simple as highlighting text and selecting the style from a drop-down menu. A user can apply a style to text, tables and presentations.

4.1.1.32 Ensures that tables are formatted consistently regarding margins, table layout and size, column widths, and font and styles.

Style Guides ensure consistent formatting for tables.

Refer to requirement 4.1.1.31 for more information regarding Style Guides.

Technical Requirements

4.1.1.33 The agency is seeking a solution that is browser based and is compatible with Microsoft Windows 10.

Wdesk is a web-based SaaS application that is browser based and compatible with Microsoft Windows 10. Workiva's recommends the latest versions of the following browsers: Google Chrome and Microsoft Edge Chromium.

5 Implementation

Workiva works closely with agencies to rapidly adapt the Wdesk platform to their existing process or new standard, and recommends a dedicated Customer Success Manager (CSM) and Solutions Architect (SA) to execute the scope of work. Upon receipt of an executed contract, your assigned CSM schedules the initial kickoff call between the agency and SA. A typical CAFR implementation takes thirty (30) to forty-five (45) days, and detailed below are the four (4) phases of implementation.

Implementation Team

Customer Success Manager (CSM)
The CSM is a trained application expert who directs day-to-day support activity for the customer, and communicates with Software Support, Product Development and other Workiva teams to ensure timely responses to customer questions, requests and incidents. The CSM is Wdesk certified and has experience working with government agencies on CAFR and budget solutions.

Solution Architect (SA)
The SA is a trained application expert responsible for executing the scope of work defined in the contract. The SA works closely with the CSM to ensure timely delivery of the project, and has extensive knowledge and experience implementing financial reporting and accounting solutions.

Connected Financial Reporting: Standard Setup Option

Standard Setup includes Document Setup and Onsite Hands-On Workshop.

Standard Document Setup: Workiva's Customer Success Team imports the agency's previously published CAFR to Wdesk, creates workbooks and documents, and links a sample set of data using best practices. Standard Document Setup allows the agency to work on their financial report immediately with continued support from the dedicated CSM.

Onsite Hands-On Workshop: Workiva's SA Team conducts a two-day onsite visit to understand how the agency's data source files integrate into the final report and to ensure the existing process or new standard is appropriately mapped in Wdesk. The SA provides process and data flow recommendations, best practices, and training as needed. In addition, the SA samples the linking feature to equip the agency to continue linking out the rest of the report.

Implementation Outline

Phase 1: Kickoff and Discovery
- Meet CSM and SA
- Review current reporting process, including current systems used for reporting and associated data
- Establish future state of reporting process using the Wdesk platform
- Finalize specific goals and expectations

- Determine detailed plan of action, including deliverables and timeline

Phase 2: Wdesk Data Setup and Configuration

- Review CAFR-related data files and other essential source data files provided by the customer
- Identify restructure needs for optimal setup
- Document setup and linking

Phase 3: Wdesk Training

- Training developed by Workiva
- Account administrator receives welcome email with access information
- Review new reporting process in configured environment
- Review spreadsheets, linking and best practices
- Finalize a go-live strategy including cut-over date for new reporting process

Phase 4: Continued Support

- Direct access training and support from CSM
- Quarterly Success Reviews (QSR) with CSM
- 24x7x365 customer support

The familiar and intuitive design of Wdesk, and a dedicated CSM ensures a smooth implementation. Agencies are comfortable with Wdesk's functionality as implementation concludes, and assured they can contact their CSM for assistance. Implementation timelines vary depending on the agency and scope of work. Workiva works closely with the agency to finalize an acceptable timeline.

Connected Financial Reporting: Wdata Setup Option

Workiva’s RFQ submission meets and exceeds the defined requirements and would look forward to entering into a partnership with the State. Over the past year, Workiva expanded setup options to include Wdata Setup. The option includes a scoping analysis with the agency, more extensive data management capabilities, and remote advisory hours, in addition to Standard Document Setup and Onsite Hand-On Training. Workiva is happy to discuss the Wdata Setup option in more detail, and why agencies choose Wdata Setup to support a variety of reporting and compliance needs.

6 Pricing Page

6.1 EXHIBIT A - Pricing Page
Option 1: Connected Financial Reporting (does not include Wdata) with Standard Setup

CONTRACT ITEM

Item #	Item	Vendor Description	Unit of Measure	Quantity	Unit Price	Extended Cost
1	Implementation and Installation	Implementation Fee for Connected Financial Reporting - Standard Setup	Lump Sum	1	$10,000.00	$10,000.00
1	First Year Maintenance and Support/Warranty/Hosting	Connected Financial Reporting	Year	1	$55,000.00	$55,000.00

CONTRACT SERVICES

Item #	Item	Vendor Description	Unit of Measure	Quantity	Unit Price	Extended Cost
2	Second Year Maintenance and Support/Warranty/Hosting	Connected Financial Reporting	Year	1	$57,750.00	$57,750.00
3	Third Year Maintenance and Support/Warranty/Hosting	Connected Financial Reporting	Year	1	$60,638.00	$60,638.00
4	Fourth Year Maintenance and Support/Warranty/Hosting	Connected Financial Reporting	Year	1	$63,670.00	$63,670.00
5	Licenses-Estimated Quantity	Connected Financial Reporting	Per License	Unlimited*	$0.00	$0.00

**Workiva's solution-based licensing (SBL) supports an unlimited number of users at no additional cost.*

7 Contract Manager

11.a 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: Chet Hayes
Telephone Number: 571.707.4137
E-mail Address: chet@vertosoft.com

8 Attachments

2019 Workiva SOC 1_ISAE3402 Report_Final.pdf
2019 Workiva SOC 2_ISAE3000_HIPPA (TSP 100) Report FINAL Updated.pdf
Workiva Master Service Level Agreement (Master Terms and Conditions.pdf)