System and Organization Controls 3 Report

Report on Management’s Description of System – Workday’s Enterprise Products Relevant to Availability, Confidentiality, Privacy, Processing Integrity, and Security

For the Period October 1, 2018 to September 30, 2019
Report of Independent Accountants

Management of Workday, Inc.

Scope
We have examined management’s assertion, contained within the accompanying Management’s Report of its Assertions on the Effectiveness of Its Controls Over the Workday’s Enterprise Products Based on the Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy (Assertion), that Workday’s controls over the Workday’s Enterprise Products (System) were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Management’s responsibilities
Workday’s management is responsible for its assertion, selecting the trust services categories and associated criteria on which the assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Workday’s Enterprise Products (System) and describing the boundaries of the System.
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Workday’s Enterprise Products (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement.

Our responsibilities
Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management’s assertion, which includes: (1) obtaining an understanding of Workday’s relevant security, availability, processing integrity, confidentiality, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we consider necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Workday’s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.
Inherent limitations

Because of their nature and inherent limitations, controls may not prevent, or detect and correct, all misstatements that may be considered relevant. Furthermore, the projection of any evaluations of effectiveness to future periods, or conclusions about the suitability of the design of the controls to achieve Workday’s principal service commitments and system requirements, is subject to the risk that controls may become inadequate because of changes in conditions, that the degree of compliance with such controls may deteriorate, or that changes made to the system or controls, or the failure to make needed changes to the system or controls, may alter the validity of such evaluations. Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity.

Opinion

In our opinion, Workday’s management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

December 18, 2019
Management’s Report of its Assertions on the Effectiveness of Its Controls over the Workday Enterprise Products System Based on the Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

We, as management of Workday, Inc. are responsible for:

- Identifying the Workday Enterprise Products (System) and describing the boundaries of the System, which are presented in Attachment A
- Identifying our principal service commitments and system requirements which are presented in Attachment A
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Workday Enterprise Products (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

Workday uses Amazon Web Services (AWS) to provide data center hosting (physical security and environmental safeguards), infrastructure support and management, and storage services. The Description (Attachment A) includes only the controls of Workday and excludes controls of AWS. The Description also indicates that certain trust services criteria specified therein can be met only if AWS’s controls assumed in the design of Workday’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS. However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents AWS from achieving its specified service commitments.

We assert that the controls over the system were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, confidentiality, and privacy set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

Barbara M Cosgrove
Barbara Cosgrove
Chief Privacy Officer
ATTACHMENT A

DESCRIPTION OF THE COMPANY

Corporate Overview

Workday is a provider of enterprise products for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, planning, and analytics applications designed for the world’s largest companies, educational institutions, and government agencies. Organizations ranging from medium-sized businesses to Fortune 50 enterprises have selected Workday.

Workday Enterprise Products encompass Workday Enterprise Cloud Applications, Workday Cloud Platform, and in-scope Workday Innovation Services defined in the section below.

Workday Enterprise Products include the following:

Human Resources – Workday’s human resource and talent management applications help organizations recruit, manage, train, organize, staff, pay, and develop a global workforce of both employees and contingent workers through the hire-to-retire process. These applications include:

- Workday Learning
- Workday Payroll
- Workday Planning (For Workforce Planning)
- Workday Recruiting
- Workday Time Tracking

Finance – Workday’s financial management applications help manage an organization’s financial accounting, reporting and management of information necessary to operate and measure the organization. In addition, these applications support the planning, budgeting, order-to-cash, revenue management, procure-to-pay, and expense management processes. These applications include:

- Workday Expenses
- Workday Financial Performance Management (FPM)
- Workday Grants Management
- Workday Planning (For Financial Planning)
- Workday Procurement
- Workday Projects

Analytics & Technology – Workday’s analytics and technology products include:

- Workday Benchmarking, an offering available as part of Workday Data-as-a-Service
Innovation Services – Applications that are available for Customers to opt in for an enhanced Workday experience. The following applications are in scope for the report as of July 1, 2019:

- Workday Graph (Skills Cloud)
- Journal Insights
- Workday Assistant
- Benchmarking

Industry specific applications:

- Workday Inventory (For Healthcare)
- Workday Professional Services Automation (For Professional Services Organizations)
- Workday Student (for Higher Education)

Technology

**Workday Architecture Overview**
Software as a Service (SaaS) – Workday delivers applications via a software as a service (SaaS) model. In this service delivery model, Workday is responsible for providing the infrastructure (i.e., hardware and middleware that comprise the Workday infrastructure), data security, software development (i.e., software updates and patches), and operational processes (i.e., operation and management of the infrastructure and systems to support the service).

Workday Private Cloud (WPC) – Workday Private Cloud (WPC) is comprised of virtualized servers running Workday services that provide enhanced scalability and flexibility of technical resources. WPC resides within Workday’s data center infrastructure.

Amazon Web Services (AWS) environments – Public Cloud, Workday Cloud Platform and the Machine Learning Development Environment are included within the scope of this report and collectively are referred to as public cloud environments. These optional environments are applicable for Customers who have opted into the respective services.

- **Public Cloud** – Workday offers Customers the option of running Workday applications in a public cloud environment hosted by AWS, utilizing AWS Elastic Compute Cloud (EC2) and Simple Storage Service (S3). Workday applications running in this environment maintain the same level of security, change management, and logical access controls.

- **Workday Cloud Platform (WCP)** – The Workday Cloud Platform enables Workday Customers and partners to build extensions and applications that run on, or integrate with, Workday. The Workday-managed components of the Workday Cloud Platform utilize AWS Elastic Compute Cloud (EC2), Simple Storage Service (S3) and AWS Lambda.

- **Machine Learning Development Environment (MLDE)** – The Machine Learning Development Environment is hosted in AWS and is used for model development to improve the functionality of Innovation Services.

The AWS environments utilized for Media Cloud (software, data, text, audio, video, images or any other content that the Customer submits as part of a learning campaign within the Workday Learning Service) and Benchmarking (non-tenanted, pseudonymized data) are not in-scope for this report.

AWS is responsible for operating, managing, and controlling various components of the virtualization layer and storage as well as the physical security and environmental controls of these environments. Controls operated by AWS are not included in the scope of this report.

The affected control objective/criteria are included below along with the expected minimum controls expected to be in place at AWS.
<table>
<thead>
<tr>
<th>Criteria</th>
<th>AWS controls expected to be in place</th>
</tr>
</thead>
</table>
| CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives. | Password and/or MFA is used to restrict access to authorized individuals.  
Encryption methods are used to protect data in transit and at rest.  
Roles and responsibilities for managing cryptographic key are formally documented.  
Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.  
Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.  
Security protections are in place to restrict access to virtual and physical devices and other information assets to authorized personnel. |
| CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized. | Additions and changes to system are authorized prior to access being granted.  
System access is removed timely upon termination. |
| CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity’s objectives. | System access is removed timely upon termination.  
System access is reviewed on a periodic basis to ensure access is restricted to authorized and appropriate individuals.  
IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning. |
<table>
<thead>
<tr>
<th><strong>Criteria</strong></th>
<th><strong>AWS controls expected to be in place</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td>CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.</td>
<td>Only authorized personnel have access to the facilities housing the system. Badge access control systems are in place in order to access the facilities. Visitor access to the corporate facility and data center are recorded in visitor access logs. Visitors are required to wear a visitor badge while onsite at the facilities. Visitors are required to check in with security and show a government issued ID prior to being granted access the facilities. Visitors are required to have an escort at all times.</td>
</tr>
<tr>
<td>CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity’s objectives.</td>
<td>All production media is securely decommissioned and physically destroyed prior to leaving the data center.</td>
</tr>
<tr>
<td>CC7.1: To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.</td>
<td>External vulnerability assessments are performed on a periodic basis, identified issues are investigated and tracked to resolution in a timely manner.</td>
</tr>
<tr>
<td>CC8.1: The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</td>
<td>Changes are authorized, tested, and approved prior to implementation.</td>
</tr>
</tbody>
</table>
| A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives. | Environmental protections have been installed including the following:  
  - Cooling systems  
  - Battery and generator backups  
  - Smoke detection  
  - Dry pipe sprinklers  
  Environmental protection equipment receive maintenance on at least an annual basis. |
Criteria | AWS controls expected to be in place
--- | ---
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives. | Backups of critical system components are monitored for successful replication across multiple data centers.

For operational processes outsourced to third parties, Workday obtains assurance through a report or certification on the effectiveness of the control environment documented by the outsourced provider’s independent auditor. Each report or certification is reviewed within 12 months of the issuance date by Workday’s Privacy, Ethics and Compliance Team, and reviews are documented using an internal tracking system. Any issues identified are evaluated based on risk and potential impact to Workday and its Customers.

**Multi-tenancy** – Multi-tenancy is a key feature of Workday. Multi-tenancy enables multiple Customers to share one physical instance of the Workday system while isolating each tenant’s (Customer’s) application data. Workday accomplishes this through the Workday Object Management Server (OMS). Every Workday account is associated with exactly one tenant, which is then used to access the Workday application. All instances of application objects (such as Organization, Worker, etc.) are tenant-based, so every time a new object is created, that object is also irrevocably linked to the user’s tenant. The Workday system maintains these links automatically, and restricts access to every object based on the user ID. The Workday system restricts access to objects based on the Workday account and tenant.

**Privacy and Security** – Workday’s privacy by design philosophy is the foundation for many privacy-enhancing features. New features are evaluated early in the development stage and throughout the entire development processes to assess and address potential privacy, security and compliance impacts. Workday employs a unified approach to security at all computing layers.

Access for end users to view or modify data within the application is only granted using a designated endpoint (e.g., web browser). Access for systems to view or modify data within the application is only granted using web services. No direct access is provided at the database layer for any end users, and every attribute value of Customer Data within the application is encrypted before it is stored. End-user access utilizes role-based security logic to authenticate the user and to make sure they have been granted a role that allows the transaction.

Workday provides non-destructive data updates for a complete audit trail of changes made to application data. When any update is made, the application records the user who made the change and the time they made the change. Reports showing system update activity by user for selected time periods are delivered with all Workday applications.

**Implementation Tools**

Workday provides various tools that facilitate implementation and configuration activities new Customer tenants or for existing Customers who have purchased additional Workday products.

Customer Central is a default additional tenant for all Workday implementations initiated after January 15, 2018. Customer Central provides Workday certified implementers access to efficiently build and maintain a Customer’s non-production tenants. Customer Central provides a centralized gateway to compare data and configuration between tenants, facilitates the migration of Workday-delivered
configuration objects from reference tenants to non-production Customer tenants, and gives implementers the ability to migrate configuration objects between non-production tenants. Non-production Customer tenants must have the opt-in setting configured to enable Customer Central access.

The scope of this report does not address actions performed by certified implementors to facilitate implementation and configuration activities.

Object Transporter (OX) is a configuration migration tool built into Customer tenants that streamlines the tenant build process by enabling implementers and Customers to migrate configuration packages and instances between Customer tenants.

CloudLoader is a data loading tool built into non-production tenants that allows implementers to import, map, cleanse (transform/validate) and load Customer implementation data. Implementers with access to a Customer’s implementation tenant can activate CloudLoader by adding the CloudLoader Worklet to their dashboard.

Customer Data

Workday defines Customer Data as the electronic data or information submitted by the Customer or Authorized Parties to the Workday Service. Customer Data is deemed confidential. Access to Customer Data is restricted to authorized personnel through the use of physical and logical access controls.

The Customer determines what data is entered into Workday applications and configures the appropriate security for the data, including who can access and use the data. Additionally, where applicable, the Customer manages any notification or consent requirements, and maintains the accuracy of the data. Workday then processes the data in accordance with its contractual agreement with the Customer and the settings implemented by the Customer.

In the normal course of operations, Customer Data exists in several environments depending on Customer needs. Environments that contain Customer Data include the following:

- Production
  - Production – Environment for the production Workday applications
- Non-Production
  - Disaster Recovery – Backup environment available for disaster recovery
  - Implementation (Deployment) – Environment used for longer-term configuration changes and testing
  - Sandbox – Environment used for testing configuration changes and training
  - Conversion Test – Verification testing for Production Customers
  - Performance – Opt-in, non-customer facing environment used for replicating performance issues
Innovation Services Data (IS Data)

Workday defines Innovation Services Data as data contributed by Customers to any specific Innovation Service. Access to Innovation Services Data is restricted to authorized personnel through the use of physical and logical access controls.

For Innovation Services that have machine learning components, Innovation Services may use the Machine Learning Development Environment (MLDE), which is hosted in AWS, for model development to improve the functionality of the Innovation Service. Customers determine what Innovation Services Data to contribute to the MLDE, and can opt out of IS Data contribution through administrative actions in the applicable Customer tenant. Innovation Services and its related machine learning components are in scope as of July 1, 2019.

Depending on the Innovation Service, Innovation Services Data may also be processed by third party subprocessor(s) applicable to the specific Innovation Service, which are listed on the Community subprocessor pages.

Workday Privacy Practices

- Workday accesses Customer Data and IS Data, in accordance with the relevant agreement between Customer and Workday.

- Workday processes Customer Data and IS Data under the direction of its Customers, and has no direct control or ownership of the personal data it processes.

- Workday retains Customer Data and IS Data according to the timeframes set forth in the relevant agreement with its Customers.

- Workday maintains a comprehensive, written information security program that contains technical and organizational safeguards designed to prevent unauthorized access to, use of or disclosure of Customer Data and IS Data.

- Workday designs its applications to allow Customers to achieve differentiated configurations, enforce user access controls, and manage data categories that may be populated and/or made accessible on a country-by-country basis.

- If required, Customers are responsible for providing notice to the individuals whose data will be collected and used within the Workday application. Workday is not responsible for providing such notice to or obtaining consent from these individuals, and is only responsible for communicating its Privacy practices to Workday’s Customers, which are included in formal agreements with the Customers.

- Workday has appointed a Chief Privacy Officer responsible for overseeing the implementation of the privacy program in the organization.

Security Program

The following table illustrates the security program components and related policies, procedures, processes, and/or control in place to address the Security Program components.
<table>
<thead>
<tr>
<th>Security Program Components</th>
<th>Relevant Policies, Procedures, Processes, and/or Controls</th>
</tr>
</thead>
<tbody>
<tr>
<td>Risk assessment and treatment</td>
<td>Information Security Management System (ISMS) Policy</td>
</tr>
<tr>
<td></td>
<td>Risk Assessment Methodology (includes Risk Treatment Plan)</td>
</tr>
<tr>
<td>Security policy</td>
<td>Workday Service Privacy Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Management System (ISMS) Policy</td>
</tr>
<tr>
<td></td>
<td>Acceptable Encryption Policy</td>
</tr>
<tr>
<td>Organization of information security</td>
<td>Workday Service Privacy Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Management System (ISMS) Policy</td>
</tr>
<tr>
<td></td>
<td>Information Security Management System (ISMS) Handbook¹</td>
</tr>
<tr>
<td>Asset management</td>
<td>Information Systems Configuration and Management Policy</td>
</tr>
<tr>
<td></td>
<td>Acceptable Use Policy</td>
</tr>
<tr>
<td></td>
<td>Mobile Device Policy</td>
</tr>
<tr>
<td>Human resources security</td>
<td>Privacy and Security Training Policy</td>
</tr>
<tr>
<td></td>
<td>Employment Background Check Policy</td>
</tr>
<tr>
<td></td>
<td>Proprietary Information and Inventions Agreement¹</td>
</tr>
<tr>
<td>Physical and environmental security</td>
<td>Job Profile Summaries¹</td>
</tr>
<tr>
<td></td>
<td>Physical Security – Hosting Facilities Policy</td>
</tr>
<tr>
<td>Access control</td>
<td>Logical Access to Workday Systems Policy</td>
</tr>
<tr>
<td></td>
<td>Password Policy</td>
</tr>
<tr>
<td></td>
<td>Remote Access Policy</td>
</tr>
<tr>
<td></td>
<td>Digital Key Management Policy</td>
</tr>
<tr>
<td>Information systems acquisition, development, and maintenance</td>
<td>Change Management Policies</td>
</tr>
<tr>
<td></td>
<td>Change Management Process Document¹</td>
</tr>
<tr>
<td></td>
<td>Handling Professional Services Data During Implementations Policy</td>
</tr>
<tr>
<td></td>
<td>Access to Customer Data Policy</td>
</tr>
<tr>
<td></td>
<td>Development/Product Management Access to Customer Data Policy</td>
</tr>
<tr>
<td>Information security incident management</td>
<td>Security Incident Policy</td>
</tr>
<tr>
<td></td>
<td>Incident Response Plan</td>
</tr>
<tr>
<td>Security Program Components</td>
<td>Relevant Policies, Procedures, Processes, and/or Controls</td>
</tr>
<tr>
<td>---------------------------------------------</td>
<td>-------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>Availability and Capacity Management</td>
<td>Database Backup Management Policy</td>
</tr>
<tr>
<td></td>
<td>Disaster Recovery Process</td>
</tr>
<tr>
<td></td>
<td>Capacity Management Process and Procedures</td>
</tr>
<tr>
<td></td>
<td>Operations Availability Metrics Process</td>
</tr>
<tr>
<td>Compliance</td>
<td>Employee Conduct and Discipline Guidelines</td>
</tr>
</tbody>
</table>

1 This document is not a formal policy document per company guidelines that requires formal review sign-offs, however the document is available to company personnel on the company intranet.

**Principal Service Commitments and System Requirements**

Workday designs its processes and procedures to meet its objectives for its Workday’s Enterprise Products. Those objectives are based on the service commitments that Workday makes to user entities, the laws and regulations that govern the provision of the Workday’s Enterprise Products, and the financial, system, operational and compliance requirements that Workday has established for the services.

Workday makes certain Availability, Confidentiality, Privacy, Processing Integrity, and Security representations to its Customers as detailed in its Master Subscription Agreement, Service Level Agreements (SLAs) and other Customer agreements, as well as in the description of the service offering provided online and within this report. Availability, Confidentiality, Privacy, Processing Integrity, and Security commitments include, but are not limited to, the following:

- Security and privacy principles within Workday’s Enterprise Products that are designed for configurable security and compliance with regulations
- Policies and mechanisms put in place to appropriately secure and segregate Customer Data
- Regular security monitoring and audits of the environment
- Use of formal HR business processes such as background checks and Security and Privacy training
- Use of encryption technologies to protect Customer Data both at rest and in transit
- Monitoring and resolution of system incidents
- Documentation, testing, authorization, and approval of Software and Operational Changes
- Maintenance and monitoring of backups to ensure successful replication to meet the service commitments
- Data integrity and availability monitoring for Production tenants and Production level platform environments
Workday establishes operational requirements that support the achievement of Availability, Confidentiality, Privacy, Processing Integrity, and Security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Workday system policies and procedures, system design documentation, and contracts with Customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of these system requirements as they relate to Workday’s Enterprise Products.

**RELEVANT ASPECTS OF INTERNAL CONTROL**

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), internal control is a process affected by an entity’s board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

- **Risk Management** – The entity’s identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.

- **Information and Communication** – Surrounding these activities are information and communication systems. These enable the entity’s people to capture and exchange information needed to conduct and control its operations.

- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

- **Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity’s control objectives are effectively carried out.

Set out below is a description of the five components of internal control as it pertains to Workday that may be relevant to Customers.

**Control Environment**

**Management Controls**

Workday management is responsible for directing and controlling operations, as well as establishing, communicating, and monitoring company-wide policies and procedures. Management places a consistent emphasis on maintaining comprehensive, relevant internal controls and on communicating and maintaining high integrity and ethical values of the Company’s personnel. Core values, key strategic elements, and behavioral standards are communicated to employees through new hire orientation, policy statements and guidelines, and regular company communications. Workday defines key security and operational roles and responsibilities as follows:
• **Chief Information Officer (CIO)** – Oversees the company’s security and global information technology (IT) organization, with responsibility for the internal deployment of business technologies and programs that create a competitive advantage for the company and serve as best practices to IT organizations globally.

• **Chief Security Officer (CSO)** – Oversees the information security program and overall security maturity of the business. This includes the identification, evaluation, and prioritization of security related risks and vulnerabilities within the Company’s product, technology and operations. The CSO is also responsible for ensuring that security risks are communicated.

• **Chief Privacy Officer (CPO)** – Responsible for promoting a culture of integrity and ethical behavior and helping Workday adhere to applicable global data protection laws, regulations, contractual commitments and privacy compliance requirements.

• **Development (including Product Management) and Quality Assurance** – Responsible for the consistent promotion and development of new products and features, including security features within Workday Enterprise Products, as well as manual and automated testing to ensure the quality of software.

• **Products & Technology Release** – Responsible for overseeing the software change management process, and holds internal weekly meetings to communicate milestones and status updates related to upcoming releases.

• **Security Council** – Workday has established a Security Council consisting of cross-functional management representatives. The Security Council meets on a quarterly basis to assess the direction and provide management support for security initiatives.

• **Platform Infrastructure and Environments Operations** – Responsible for the administration and monitoring of user access to Workday’s internal systems, administration and management of application, persistent data store, database, and operating system availability, where applicable.

• **Support** – Workday’s Support team is designed to respond to and collaborate with Customers when they believe Workday Enterprise Products are not operating as designed.

• **Internal Audit** – Provides an independent and objective assessment of Workday’s internal risk management program and internal controls frameworks to validate that the Company is operating effectively and as designed.

**Personnel Policies and Procedures**

Workday employs people who are selected and valued for their intuition, intelligence, integrity and passion for delivering superior solutions to Customers. The Company’s Human Resources, Security, and Privacy, Ethics and Compliance team, together with Management, are responsible for developing, maintaining, and communicating company policies and procedures that promote Workday’s core values.

**Risk Management**

Financial, IT, and relevant industry risks are periodically assessed and reviewed by Workday senior management. Company policies and procedures focused on risk management within the Company, as well as acceptable usage and other security related areas of focus, are maintained, updated, and
communicated to employees on a regular basis. These policies and procedures are also available to Workday employees on the company intranet.

On an annual basis, a formal risk assessment is performed by the Privacy, Ethics and Compliance team as part of the ISO27001 Information Security Management System (ISMS) requirements. The risk assessment is performed by using the Workday ISO27001 risk assessment as a basis for risk identification, with additional risks that threaten the achievement of the control objectives added, as appropriate. As part of this process, threats to security, confidentiality, availability, and integrity of Customer Data and threats to the privacy and protection of personal data provided as Customer Data are identified and the risks from these threats are formally assessed. Based on the risk assessment, program changes are made, as necessary, and the Privacy, Ethics and Compliance team monitors the effectiveness of the associated programs, including the Privacy program.

Additionally, external network, system, and application vulnerability threat assessments are performed by third party security service providers on a periodic basis. The results of these assessments are reviewed by Workday senior management, including the Chief Security Officer. Issues noted are assessed for criticality and severity, and assigned to the appropriate resources for remediation.

In addition, Workday maintains cyber risk insurance to offset the impact of loss events that would otherwise impair the ability of the entity to meet its objectives.

**Information and Communication**

Management is committed to maintaining effective communication with all personnel, Customers and business partners. Issues or suggestions identified by Workday personnel are promptly brought to the attention of management to be addressed and resolved.

To help align Workday’s business strategies and goals with operating performance for its Customers, the Company’s Products & Technology Release Team has established appropriate communication methods and periodic meetings to review status and issues related to upcoming releases. Workday documents and shares internal content using web-based documentation repositories and issue tracking tools.

The Company regularly posts information about product enhancements in the Workday Community. The Community contains information to assist Customers with Workday Enterprise Products. The content is searchable, and the Workday Community site includes the following:

- Current Workday company and application news and events
- Relevant information to help users understand, navigate, and use Workday Enterprise Products
- Link to login to the support site where Customers are able to ask questions and report problems

**Monitoring**

The Infrastructure and Environments Operations teams are responsible for monitoring the effectiveness of internal controls in the normal course of operations. Deviations in the operation of internal controls, including major security, availability and processing integrity events, are reported to senior management. In addition, any prospect or Customer issues are communicated to the appropriate Workday personnel.
using a web-based issue tracking tool. Workday employees can monitor the status of the issue tickets, and are notified when changes occur.

In order to provide the basis for Management’s Assertion on the design and operating effectiveness of controls created to achieve the related criteria, the Privacy, Ethics and Compliance team performs inquiry of each control owner and/or operator and reviews documentation provided by management which support the achievement of each control objective.

An internal issue remediation and improvement opportunity procedure exists to track areas of remediation and/or improvement identified from external compliance assessments. Within this process, Workday performs root cause analysis, assigns follow-up action items and owners to track remediation where appropriate.

Workday also uses automated tools and systems to monitor the security and availability of the Enterprise Products, including network, application, database, persistent data store, and operating system activities. In addition, system and access logs are maintained for critical systems to support monitoring investigations and resolution, as necessary.

Appropriate contact with special interest groups and law enforcement authorities is maintained to support broader cybersecurity situational awareness.