System and Organization Controls 3 Report

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

For the Period October 1, 2020 to September 30, 2021

Management's Report of its Assertions on the Effectiveness of Its Controls over the Workday Enterprise Products 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 infrastructure-as-a-service services. The boundaries of the System presented in Attachment A includes only the controls of Workday and excludes controls of AWS. However, the description of the boundaries of the system does present the types of controls Workday assumes have been implemented, suitably designed, and operating effectively at AWS. Certain trust services criteria 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 Workday. 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 us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period October 1, 2020 to September 30, 2021, 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,* if the subservice organization applied the controls assumed in the design of Workday's controls throughout the period October 1, 2020 to September 30, 2021.

Workday, Inc.

Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA 94105-2907

Tel: +1 415 894 8000
Fax: +1 415 894 8099
ey.com

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 Enterprise Products Based on the Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy (Assertion), that Workday's controls over the Workday Enterprise Products (System) were effective throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, confidentiality, processing integrity, 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.

Workday uses Amazon Web Service (AWS) (subservice organization) to provide infrastructure-as-a-service services. The Description of the boundaries of the System (Attachment A) indicates that Workday's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS's controls, assumed in the design of Workday's controls, are suitably designed and operating effectively along with related controls at the service organization. The description of the boundaries of the system presents Workday's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our examination did not extend to the services provided by AWS and we have not evaluated whether the controls management assumes have been implemented at AWS have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2020 to September 30, 2021.

Management's responsibilities

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

- Identifying the System and describing the boundaries of the System
- Identifying our 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 our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the 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, confidentiality, processing integrity, and privacy policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered 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 controls over the System were effective throughout the period October 1, 2020 to September 30, 2021, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the applicable trust services criteria if the subservice organization controls assumed in the design of Workday's controls operated effectively throughout the period October 1, 2020 to September 30, 2021.

Ernst & Young LLP

January 5, 2022

ATTACHMENT A - CORPORATE OVERVIEW AND SCOPE OF SERVICES

A. WORKDAY OVERVIEW

Workday is a provider of enterprise cloud applications for finance and human resources. Founded in 2005, Workday delivers applications for financial management, human resources, planning, spend management, and analytics to thousands of organizations around the world and across industries. Organizations ranging from medium-sized businesses to Fortune 50 enterprises have selected Workday.

Workday Enterprise Products encompass the following:

In-scope Workday Enterprise Products (Core Service, Workday Media Cloud, Workday Extend, Innovation Services)	
Enterprise Products	**Description**
Human Capital Management Talent Management Payroll and Workforce Management	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. • Human Capital Management • Talent Optimization • Payroll for US • Payroll for Canada • Payroll for UK • Payroll for France • Cloud Connect for Third Party Payroll • Cloud Connect for Benefits • Time Tracking • Recruiting • Learning • Learning for Extended Enterprise
Financial Management Spend Management Professional Services Automation	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. • Core Financials • Accounting Center • Expenses • Procurement • Inventory • Grants Management

In-scope Workday Enterprise Products (Core Service, Workday Media Cloud, Workday Extend, Innovation Services)	
Enterprise Products	**Description**
	• Projects • Project Billing Note: Report coverage does not include Workday Strategic Sourcing, which is addressed in the Workday Strategic Sourcing SOC audit report.
Enterprise Planning	Financial, workforce, sales planning, as well as analytics for the entire enterprise. • HCM Planning • Financials Planning • Financial Performance Management Note: Report coverage does not include Workday Adaptive Planning, which is addressed in the Workday Adaptive Planning SOC audit report.
Analytics and Reporting	Financial, workforce and operational analytics, and data management. • Workday Prism Analytics
Student	Workday Student supports academic institutions in student recruiting, student application processing and admissions, managing courses, programs, enrollment and student records, academic advising, tracking financial aid, and managing student financial accounts. Workday Student includes dashboards and reports to support institutional effectiveness.
Platform and Product Extensions	Solutions for extensibility, including application development and integrations. Workday Extend – Allows customers to build custom applications alongside existing Workday products. Workday Success Plans (supported by Workday Credentials) – Provides guidance from Workday experts to help Customers troubleshoot configuration issues, provide advice on how to configure Workday to meet business requirements, and explore Workday product features. Workday Media Cloud (WMC) – Supports the upload, sharing, and playback of rich media to provide customers with an engaging, consumer-like experience across a variety of Workday applications, including Learning, Recruiting, Dashboard Announcements, People Experience, and more. Innovation Services – Products and services which enhance and optimize a Customer's experience and are made available under the Innovation Services Agreement. The following are in scope for the report:

In-scope Workday Enterprise Products (Core Service, Workday Media Cloud, Workday Extend, Innovation Services)	
Enterprise Products	**Description**
	• Public Data • Advanced Benchmarks (as part of Workday DaaS) • Workday Graph (Skills Cloud) • Journal Insights • Workday Assistant • Benchmarking • Natural Workspaces • HCM Machine Learning Generally Available Features • Learner Name • Notification Designer • Workday Journeys • Content Cloud • User Experience Machine Learning for Available Services • Workday Help • Spend Management ML

In-scope Environments	
Enterprise Products	**Description**
Co-location Data Centers	Ashburn, Virginia • Equinix (No longer in use as of August 31, 2021) • Digital Realty Trust • Sabey (As of December 5, 2021) Hillsboro, Oregon • Flexential • Quality Technology Services (QTS) Dublin, Ireland • Digital Realty Trust Atlanta, Georgia • Quality Technology Services (QTS) Amsterdam, Netherlands • Equinix Ontario, Canada • Equinix

In-scope Environments	
Enterprise Products	**Description**
Public Cloud (Amazon Web Services)	Workday offers Customers the option of running Workday applications in a public cloud environment hosted by AWS. Additionally, extended products and services such as Workday Extend, Machine Learning Development Environment (MLDE), Workday Media Cloud (WMC), Innovation Services (Natural Workspaces, Benchmarking) are also hosted in AWS. The following AWS regions are in scope: • AWS Canada (Central), ca-central-1 • AWS EU West (Ireland), eu-west-1 • AWS US West (Oregon), us-west-2 • AWS US East (Ohio), us-east-2 • AWS Asia Pacific (Singapore), ap-southeast-1

Technology

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).

Multi-tenancy – Multi-tenancy is a key feature of the Workday Core Service. 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 – The Company'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. The Company employs a unified approach to security at all computing layers.

Hosting Environments – Amazon Web Services is utilized as an optional Infrastructure-as-a-Service provider hosting the environments applicable for Customers who have opted into the relevant services as described above. 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 criteria are included below along with the minimum controls expected to be in place at the aforementioned hosting provider:

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
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.	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
	VPC-Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.
	KMS-Specific – Roles and responsibilities for KMS cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities change.
	KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account.
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.	IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.
	User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
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.	IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.
	User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.
	IT access privileges are reviewed on a periodic basis by appropriate personnel.

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
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.	Physical access to data centers is approved by an authorized individual.
	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
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.	All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.
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.	AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.
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.	AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service.
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.	Amazon-owned data centers are protected by fire detection and suppression systems.
	Amazon-owned data centers are air-conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owner data centers.
	Amazon-owned data centers have generators to provide backup power in case of electrical failure.

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
A1.2: (continued)	Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.
	AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
	Objects are stored redundantly across multiple fault-isolated facilities.
	The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
	If enabled by the customer, RDS backs up customer databases, stored backups for user-defined retention periods, and supports point-in-time recovery.

B. 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 the MSA, 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 the Service that are designed for configurable security and compliance with regulations.
- Policies and mechanisms put in place to appropriately secure and separate Customer Data.
- Regular security monitoring and audits of the environment.

- Use of formal HR business processes such as background checks and Security and Privacy trainings.
- 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 Enterprise Products.

C. Availability and Processing Integrity

Operations teams are responsible for tracking and analyzing the availability of the Service for all customers in Production data center environments. Service availability metrics are reviewed by management on a quarterly basis. The process includes aggregation of the customer availability data on a monthly basis and comparison of that data to contractually-required Service Level Agreements (SLAs). This process also includes a monthly qualitative review based on the findings from activities that have an impact on the availability of the Service.

D. Confidentiality

Signed nondisclosure agreements are required before information designated as confidential is shared with third parties. Workday maintains privacy and confidentiality practices in accordance with contractual obligations.

The Company does not, in the normal course of business, disclose Personal Data provided to the Company to third parties.

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 on an annual basis by the Technology Compliance team, and reviews are documented using an internal tracking system. Security and privacy

considerations are evaluated during the vendor contracting process. Any issues identified are evaluated based on risk and potential impact to the Company and its Customers.

The Company maintains privacy and confidentiality practices in accordance with contractual obligations. If privacy and confidentiality practices are materially lessened, customer consent is obtained prior to implementing the less restrictive practices.

E. Privacy and Security

Privacy by Design and Privacy by Default principles are closely tied to Workday's core values and guide how Workday builds products, develops software, and operates services. In providing its Service, Workday has implemented policies and procedures that comply with global data protection laws and regulations. Detailed review by the Privacy and Compliance teams helps ensure products and releases adhere to applicable laws and requirements as well as internal documented policies and procedures. All major application releases are approved by the Chief Privacy Officer before moving to production, representing that Workday develops and designs its Service in conjunction with established Privacy by Design and Privacy by Default principles. In addition, Workday makes information available to its customers through Community to support their ability to complete their own data protection impact assessments (DPIAs).

Workday Privacy Practices

The following privacy practices are in place at the Company:

- Workday will only access 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 provides documentation to Customers explaining the types of security measures available to protect Customers' individual personal 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 interacts with the Customer based upon contractual agreements, and not with individuals providing personal data.

- Significant changes to Workday's standard customer-facing data processing terms require management approval.

- Workday has appointed a Chief Privacy Officer with responsibility, authority and accountability for monitoring a Privacy Program that is designed to adequately protect Personal Data that is provided to Workday as Customer Data and to meet the requirements of applicable Data Privacy and Protection laws and regulations. In addition, Workday's Data Protection Officer oversees data privacy compliance and manages data protection risk for the organization. Workday has a global Privacy team responsible for the operations and maintenance of the privacy program.

- A third party performs an annual review of Workday's privacy practices to confirm that they are consistent with Workday's customer-facing privacy policies.

Security Program

The following table illustrates the security program components, related policies, procedures, processes, and/or control in place at Workday to address the component:

Security Program Component	Relevant Policy, Procedure, and/or Process
Risk Assessment and Treatment	Information Security Management Systems Policy
	Security Risk Assessment Policy
	Privacy Information Management Systems (PIMS) Policy
	Security Risk and Governance Policy
	Information Security Management System Handbook[1]
	Risk Assessment Methodology (includes Risk Treatment Plan)
Security Policy	Information Systems Configuration and Management Policy
	Acceptable Encryption Policy
	Security Solutions Policy
	Network Security Policy
Organization of Information Security	Workday Privacy Statement[1]
Asset Management	Mobile Device Management Policy
	Acceptable Use Policy
	BYOD Policy
	Security – Media Disposal and Reuse Policy
	Meeting Recording and Display Policy
Human Resources Security	Employment Background Check Policy
	Proprietary Information and Inventions Agreement (PIIA)[1]
	Employee Conduct and Discipline Guidelines[1]

Security Program Component	Relevant Policy, Procedure, and/or Process
	Employment Privacy Statement[1]
	Electronics and Communications Policy
	Job Profile Summaries[1]
Physical and Environmental Security	Physical Security – Hosting Facilities Policy
Access Control	Identity and Access Management Policy
	Digital Key Management Policy
Information Systems Acquisition, Development, and Maintenance	Information Classification Policy
	Workday Vendor Risk Management Policy
	Development/Product Management Access to Customer Data Policy
	Handling Professional Services Data During Implementations Policy
	Privacy and Information Security Training Policy
	Access to Customer Data Policy
	Workday Customer Data Privacy Policy
	Change Management Policy
	Workday Software Change Management Process[1]
	Workday Operations Change Management Process[1]
Information security incident management	Incident Response Plan[1]
	Security Incident Management Policy
	Security Vulnerability Management Policy
Availability and Capacity Management	Database Backup Management Policy
	Disaster Recovery Plan[1]
	Capacity Management Process and Procedures
	Operations Availability Metrics Process[1]
Compliance	Workday Internal Privacy Policy
	Government Data Request Policy
	Meeting Recording and Display Policy

[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.

F. CONTROL ENVIRONMENT

Management Controls

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:

Personnel Policies and Procedures

The Company 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, Privacy, and Technology Compliance teams, together with Management, are responsible for developing, maintaining, and communicating company policies and procedures that promote Workday's core values.

Risk Management

Financial, IT, security, privacy, 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 and Technology Compliance teams 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 and Technology Compliance teams monitor the effectiveness of the associated programs, including the Privacy program.

Information and Communication

Management is committed to maintaining effective communication with all personnel, Customers, and business partners. Issues or suggestions identified by Company 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 and 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 on Workday Community. Workday Community contains information to assist Customers with Workday Enterprise Products.

Monitoring

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 Customer issues are communicated to the appropriate personnel using a web-based issue tracking tool.