# System and Organization Controls (SOC) 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, 2022 to September 30, 2023

## 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 (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 our 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 requirements
- Selecting the trust services categories and associated criteria that are the basis of our assertion

Workday, Inc. uses Amazon Web Services (AWS) to provide data center hosting (physical security and environmental safeguards), infrastructure support and management, and storage services. The description of the boundaries of the system presented in Attachment A indicates that complementary controls at AWS that are suitably designed and operating effectively are necessary, along with controls at Workday, Inc. to achieve the service commitments and system requirements. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of Workday, Inc.'s controls. It does not disclose the actual controls at AWS.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the trust services 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* ( *With Revised Points of Focus – 2022*).

**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

# Independent Service Auditor's Report

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, Inc.'s controls over the Workday Enterprise Products System (System) were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that Workday, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, confidentiality, and privacy (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)*.

Workday, Inc. uses Amazon Web Services (AWS) (Subservice Organization) to provide data center hosting (physical security and environmental safeguards), infrastructure support and management, and storage services. The Description of the boundaries of the System (Attachment A) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with related controls at Workday, Inc., to provide reasonable assurance that Workday, Inc.'s service commitments and system requirements are achieved based on the applicable trust service criteria. The description of the boundaries of the system presents the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS. Our procedures 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, 2022 to September 30, 2023.

*Management's responsibilities*

Workday, Inc.'s management is responsible for its service commitments and system requirements, and for designing, implementing, operating, and monitoring effective controls within the system to provide reasonable assurance that Workday, Inc.'s service commitments and system requirements were achieved. Workday, Inc. management is also responsible for providing the accompanying assertion about the effectiveness of controls within the system, selecting the trust services categories and associated criteria on which its assertion is based, and having a reasonable basis for its assertion. Management is also responsible for:

- Identifying the System and describing the boundaries of the System
- Identifying the service commitments and system requirements and the risks that would threaten the achievement of the principal service commitments and service requirements that are the objectives of the System.

Building a better working world

*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 AICPA. 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, Inc.'s relevant security, availability, and confidentiality 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, Inc.'s cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.

We are required to be independent of Workday, Inc. and to meet our other ethical responsibilities, as applicable for examination engagements set forth in the Preface: Applicable to All Members and Part 1 – Members in Public Practice of the Code of Professional Conduct established by the AICPA.

*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, Inc.'s 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, Inc.'s controls over the System were effective throughout the period October 1, 2022 to September 30, 2023, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

January 10, 2024

## ATTACHMENT A - CORPORATE OVERVIEW AND SCOPE OF SERVICES

## A. WORKDAY SYSTEMS OVERVIEW

Workday, Inc. ("Workday" or "the Company"), headquartered in Pleasanton, California, is a provider of enterprise cloud applications for finance and human resources, helping customers adapt and thrive in a changing world. Workday applications for financial management, human resources, planning, spend management, and analytics help organizations around the world embrace the future of work. Workday is used by more than 10,000 organizations around the world and across industries – from medium-sized businesses to more than 50% of the Fortune 500.

Workday is committed to protecting Customer Data/Customer Content and communicating transparently. Workday employs measures across our people, processes, and technology to ensure that Customer Data/Customer Content, applications, and infrastructure remain safe.

### Service Description and Report Scope

The scope of this report encompasses Workday Enterprise Products, which include the following:

| **In-Scope Services** | | |
|---|---|---|
| Human Capital Management | Product SKUs | Advanced Compensation Management |
| | | Benefits |
| | | Cloud Connect for Benefits |
| | | Core Human Capital Management |
| | | Help |
| | | Journeys |
| | | Human Capital Management |
| | | Onboarding |
| | Innovation Services/Enhanced Features | Help |
| | | Journeys |
| Financial Management | Product SKUs | Accounting Center |
| | | Core Financials |
| | | Expenses |
| | | Financial Management Connector for Salesforce |
| | | Financial Performance Management |

| In-Scope Services | | |
|---|---|---|
| | | Grants Management |
| | | Project Billing |
| | | Projects |
| | | Revenue Management |
| | | Time Tracking |
| | Innovation Services/Enhanced Features | Financial Management ML GA Features |
| | | Receipt Scanning for Expenses |
| | | Supplier Invoice Automation - Scanning |
| | | Distance Calculation for Expenses |
| Student | Product SKUs | Workday Student Service |
| | Innovation Services/Enhanced Features | - |
| Spend Management | Product SKUs | Inventory |
| | | Procurement |
| | Innovation Services/Enhanced Features | Spend Management ML |
| Payroll | Product SKUs | Cloud Connect for Third Party Payroll |
| | | Payroll for Canada |
| | | Payroll for France |
| | | Payroll for United Kingdom |
| | | Payroll for United States |
| | Innovation Services/Enhanced Features | - |

| In-Scope Services | | |
|---|---|---|
| Workforce Management | Product SKUs | Absence Management |
| | | Time Tracking |
| | | Time Tracking Hub |
| | | Scheduling |
| | | Labor Optimization |
| | Innovation Services/Enhanced Features | Workforce and Pay ML |
| Talent Management | Product SKUs | Learning |
| | | Cloud Connect for Learning |
| | | Recruiting |
| | | Succession Planning |
| | | Talent Optimization |
| | | Workday Learning for Extended Enterprise |
| | | Career and Development Planning |
| | | Performance and Goals |
| | | Performance and Development |
| | | Candidate Engagement |
| | Innovation Services/Enhanced Features | Human Capital Management ML GA Features |
| | | Cloud Connect for Learning |
| | | Public Learning Content |
| | | Learner Name |
| | | Recommended Interview Scheduling |
| Analytics and Reporting | Product SKUs | People Analytics |
| | | Prism Analytics |
| | Innovation Services/Enhanced Features | People Analytics |
| | | Human Capital Management ML GA Features |

| In-Scope Services | | |
|---|---|---|
| Adaptive Planning | Product SKUs | Operational Planning |
| | | Sales Planning |
| | | Planning |
| | Innovation Services/Enhanced Features | - |
| Platform and Product Extensions | Product SKUs | Extend |
| | | Messaging |
| | | Media Cloud |
| | | Data-as-a-Service - Benchmarking |
| | | Workday Success Plans |
| | Innovation Services/Enhanced Features | User Experience Machine Learning for Available Services |
| | | Workday Assistant |
| | | Global Address Lookup |
| | | Notification Designer |
| | | Workday Graph |
| | | Benchmarking, including Advanced Benchmarks |
| | | Public Data |
| | | Workday Everywhere |
| | | Email Analytics |
| | | Email Ingestion |

| In-Scope Environments | |
|---|---|
| Co-location Data Centers | **U.S Region**<br>**Ashburn, Virginia (WD1)**<br>• Digital Realty Trust<br>• Sabey<br>**Atlanta, Georgia (WD2)**<br>• Quality Technology Services (QTS)<br>**Hillsboro, Oregon (WD5)**<br>• Flexential<br>• Quality Technology Services (QTS) |
| | **EU Region**<br>**Dublin, Ireland (WD3)**<br>• Digital Realty Trust<br>**Amsterdam, Netherlands (WD3)**<br>• Equinix<br>• Serverfarm |
| | **CAN Region**<br>**Ontario, Canada**<br>• Equinix |
| Public Cloud | 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), Automated Training Environment (ATV), Machine Learning Platform Clusters (MLPC), Workday Media Cloud (WMC), and certain Innovation Services/Enhanced Features (Workday Everywhere, Benchmarking) are also hosted in AWS. The following AWS regions are in scope:<br>• AWS Canada (Central), ca-central-1<br>• AWS EU West (Ireland), eu-west-1<br>• AWS EU Central (Frankfurt), eu-central-1<br>• AWS US East (Ohio), us-east-2<br>• AWS US West (Oregon), us-west-2<br>• AWS Asia Pacific (Singapore), ap-southeast-1<br>• AWS Asia Pacific (Sydney), ap-southeast-2 |

**Architecture**

***Software as a Service (SaaS)***

Workday delivers its 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), 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 Workday Enterprise Products. 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 application restricts access to objects based on the Workday account and tenant.

When a user requests data, the system automatically assigns the request to one and only one tenant to ensure that it retrieves only information corresponding to the user's tenant. There is a single request method to access data through the OMS. Each request requires a tenant – the OMS does not allow "tenantless" requests. Each request requires authentication and authorization, which is tied to a specific tenant and user session. Once authenticated, all requests must have a valid session ID unique to the tenant, which cannot be used to access any other tenant.

**Hosting Environments**

The Workday application and Customer tenants are hosted in co-location data center facilities and/or a public cloud service provider(s). Workday offers Customers the option of running Workday applications in a Public Cloud environment hosted on Amazon Web Services (AWS). Portions of Workday Extend, Media Cloud, Benchmarking, the Machine Learning Development Environment (MLDE), the Automated Training Environment (ATV), the Machine Learning Platform Cluster (MLPC) environment, and other Innovation Services/Enhanced Features are also hosted on AWS. Sub-service Organizations and Complementary Subservice Organization Controls (CSOCs).

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 sub-service organization:

| Sub-service Organization Controls | |
|---|---|
| **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 Controls | |
|---|---|
| **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 verified by two personnel, 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-owned data centers and third-party colocation sites where Amazon maintains the UPS units. |
| | Amazon-owned data centers have generators to provide backup power in case of electrical failure. |

| Sub-service Organization Controls | |
|---|---|
| **Criteria** | **Control** |
| **A1.2 (cont'd)** | 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 (unless maintained by Amazon), 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. | S3-Specific - When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy. |
| | S3-Specific - Objects are stored redundantly across multiple fault-isolated facilities. |
| | S3-Specific - The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service. |
| | RDS-Specific - If enabled by the customer, RDS backs up customer databases, stored backups for user-defined retention periods, and supports point-in-time recovery. |

**Implementation Tools**

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

Customer Central is a default additional tenant for all Workday implementations. 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.

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.

Configurable logical access security within Customer Central follows Workday's standardized security framework. Implementer accounts must exist in the target implementation tenants to enable access from Customer Central. Implementer access to CloudLoader and Object Transporter occurs through a Customer's implementation tenant and is provisioned/removed via Workday's standardized implementer tenant access management process.

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

## B. Principal Service Commitments and System Requirements

Workday designs its processes and procedures to meet its objectives for Workday Enterprise Products. Those objectives are based on the service commitments that Workday makes to user entities based on, among others, the trust services criteria for security, availability, confidentiality, processing integrity, and privacy, the National Institute of Standards and Technology (NIST) Cybersecurity Framework (NCF) criteria, the NIST 800-171 criteria, and NIST Privacy Framework (NPF) criteria, as well as the laws and regulations that govern the provision of Workday 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 Content.
- 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 Content 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.

The processing integrity of Workday-delivered reports are covered in Workday's comprehensive Software Delivery process. This includes both manual end-to-end and automated Quality Assurance (QA) testing. Test procedures include, but are not limited to, data input/validation, recalculation, user interface, and security, to ensure functional design, completeness, and accuracy. For the Workday application, system validation occurs on data input into the application based on attribute type.

## 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 high risk 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 Third Party Security team as part of the Ongoing Monitoring Process, and reviews are documented using an internal tracking system. Any issues identified are evaluated based on risk and potential impact to the Company and its Customers.

Workday 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 Program

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 several teams help 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 Workday Community to support their ability to complete their own data protection impact assessments (DPIAs).

### Security Program

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 Content. Workday provides documentation to Customers explaining the types of security measures available to protect Customers' individual personal data.

## F. Control Environment

### Leadership and Management

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.

### Personnel Security

#### *Hiring Practices*

Integrity and high ethical standards are fundamental values to Workday. Workday employs people who are selected for their intuition, intelligence, integrity, and passion for delivering solutions to Customers. Employment candidates are evaluated by Workday to determine whether their skills and experience are a fit for the Company prior to hire.

### Enterprise Risk Management

Financial, IT, security, privacy, and other relevant industry risks are periodically assessed and reviewed by Workday management. Workday maintains policies and procedures focused on risk management.

On an annual basis, a formal risk assessment is performed by Workday as part of the ISO27001 certified Information Security Management System (ISMS) requirements. The risk assessment is performed by using the Workday ISMS risk assessment methodology 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 Content, and threats to the privacy and protection of personal data provided as Customer Content, are identified and the risks from these threats are formally assessed.

Based on the risk assessment, program changes are made as necessary, and appropriate teams monitor the effectiveness of the associated programs.

In addition, Workday maintains cyber risk insurance.

**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**

Workday has designated teams 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.