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, 2024 to September 30, 2025

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 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 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) and Google Cloud Platform (GCP) to provide data center hosting (cloud computing infrastructure), 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 and GCP 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 and GCP.

We confirm to the best of our knowledge and belief that the controls over the System were effective throughout the period October 1, 2024 to September 30, 2025, 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 in AICPA *Trust Services Criteria*.

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

To the Board of Directors 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, Processing Integrity, Confidentiality, and Privacy (Assertion), that Workday, Inc.'s controls over the Workday Enterprise Products (System) were effective throughout the period October 1, 2024 to September 30, 2025, 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, in AICPA Trust Services Criteria*.

Workday, Inc. uses Amazon Web Services (AWS) and Google Cloud Platform (GCP) (collectively, Subservice Organizations) to provide data center hosting (cloud computing infrastructure), infrastructure support and management, and storage services. The description of the boundaries of the system presented at 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 and GCP. Our procedures did not extend to the services provided by AWS and GCP and we have not evaluated whether the controls management assumes have been implemented at AWS and GCP have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2024 to September 30, 2025

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. It 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 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, 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 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.

Our examination procedures were limited to certain aspects of the AI services, to the extent needed to obtain evidence that the service commitments and system requirements were achieved based on the relevant trust services criteria. This did not include all of the AI services that Workday operates, nor all of the aspects of the AI services for which we performed procedures.

The AI services and related applications are inherently designed to learn and adapt over time. This adaptability introduces variability in their behavior and outputs. As AI services evolve based on new data and interactions from user entities, the decision-making processes are subject to change, which can impact the completeness, validity, and accuracy of the output.

Moreover, the completeness, validity, and accuracy of the AI services output is significantly influenced by the quality of the underlying data, and the outputs are context specific. The data is owned and managed by the user entities, and any inconsistencies or biases in the data, as well as the context provided by user entities can directly influence the completeness, validity, and accuracy of the AI services. Accordingly, we do not express an opinion on the completeness, validity, and accuracy of the AI services.

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, 2024 to September 30, 2025, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria.

Ernst & Young LLP

December 2, 2025

ATTACHMENT A - CORPORATE OVERVIEW AND SCOPE OF SERVICES

A. WORKDAY SYSTEMS OVERVIEW

Workday, Inc. ("Workday" or "the Company"), headquartered in Pleasanton, California, is an enterprise platform that helps organizations manage human resources and finances. Workday is used by more than 11,000 organizations around the world and across industries – from medium-sized businesses to more than 65% of the Fortune 500.

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

The Workday Enterprise Products covered in the Service Description and Report Scope section includes Workday Core and Adaptive Planning products.

Service Description and Report Scope

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

In-Scope Workday Core Products and Services		
Human Capital Management (HCM)	**Product SKUs**	Advanced Compensation Management-LDP
		Benefits- LDP
		Cloud Connect for Benefits
		Core Human Capital Management
		Help
		Journeys
		Human Capital Management
		Talent Optimization
	Innovation Services	Help
		Journeys
		Ad Hoc Worker Communications
Financial Management	**Product SKUs**	Accounting Center
		Auditoria.AI SmartBots for Workday
		Core Financials
		Expenses
		External Transaction Matching

In-Scope Workday Core Products and Services		
		Financial Management Connector for Salesforce
		Financial Performance Management
		Grants Management
		Project Billing
		Projects
		Services CPQ
		Revenue Management- LDP
		Time Tracking
		Workday Bank Connectivity
		Workday Bank Connectivity Payment Entitlement
	Innovation Services	Auditoria.AI SmartBots for Workday
		Distance Calculation for Expenses
		Financial Management ML GA Features
		Receipt Scanning for Expenses
		Supplier Invoice Automation - Scanning
		Workday Bank Connectivity
Student	**Product SKUs**	Workday Student Service
	Innovation Services	N/A
Spend Management	**Product SKUs**	Inventory
		Procurement
	Innovation Services	Spend Management ML
Payroll	**Product SKUs**	Cloud Connect for Third Party Payroll
		Global Payroll Connect
		Payroll for Canada
		Payroll for France
		Payroll for United Kingdom
		Payroll for United States

In-Scope Workday Core Products and Services		
		Payroll for Australia
		Payroll provided by Strada
	Innovation Services	Payroll Machine Learning Generally Available Features
		P45 Tax Form Scanning
Workforce Management	**Product SKUs**	Absence Management
		b-comm Time Clock Connector provided by dormakaba
		Time Tracking Hub
		Scheduling
		Smart Time Clock
		Labor Optimization
	Innovation Services	Workforce and Pay ML
Talent Management	**Product SKUs**	Learning
		Cloud Connect for Learning
		Recruiting
		Succession Planning
		Talent Optimization
		Talent Optimization Add On
		Workday Learning for Extended Enterprise
		Performance and Development
		Candidate Engagement
	Innovation Services	Human Capital Management ML GA Features
		Cloud Connect for Learning
		Talent Optimization
		Public Learning Content
		Learner Name
		e-Commerce for Learning
		Recommended Interview Scheduling
Analytics and Reporting	**Product SKUs**	People Analytics
		Prism Analytics

In-Scope Workday Core Products and Services		
	Innovation Services	People Analytics
Platform and Product Extensions	**Product SKUs**	Bring Your Own Key
		Extend
		Media Cloud
		Messaging
		Workday Cloud Platform
		Workday Government Cloud
	Innovation Services	User Experience Machine Learning for Available Services
		Workday Assistant
		Workday Graph
		Workday Everywhere
		Email Analytics
		Email Ingestion
		Intelligent Core
		SMS Multi-Factor Authentication
		Enterprise Search
		Workday AI Gateway
		Workday Orchestrate for Integrations
		Productivity Suite ML Features
		Global Address Validation
		Messaging
		Extend Integration with Third Party Platform Services
		Global Address Lookup
		Notification Designer

In-Scope Adaptive Planning Products and Services		
Adaptive Planning	**Product SKUs**	Financial Planning
		Operational Planning
		Planning
		Workforce Planning
	Innovation Services	N/A

In-Scope Workday Environments		
Environment	Co-location Data Centers: Workday Core (WD)	U.S. Region WD1 - Ashburn, Virginia • Sabey WD2 - Atlanta, Georgia • Quality Technology Services (QTS) WD5 - Hillsboro, Oregon • Flexential • Quality Technology Services (QTS)
		EU Region WD3 - Dublin, Ireland • Digital Realty Trust • Pure WD3- Amsterdam, The Netherlands • Serverfarm
	Public Cloud: **Workday Core (WD) and Adaptive Planning (AP)**	U.S. Region • WD12 (AWS us-east-2) • WD12 (AWS us-west-2) • WD104 (AWS us-east-2) • WD104 (AWS us-west-2) • WD107 (AWS eu-west-2) • WD108 (AWS us-east-2) • WD501 (GCP us-east) • WD501 (GCP us-west1) • WD503 (GCP us-east-1) • AP (AWS us-east-1) • AP (AWS us-west-2)

In-Scope Workday Environments		
		EU Region • WD103 (AWS eu-central-1) • WD502 (GCP eu-west-1) • WD10 (AWS eu-west-1) • WD107 (AWS eu-west-2)
		APJ Region • WD102 (AWS ap-southeast-1) • WD105 (AWS ap-southeast-2) • AP (AWS ap-southeast-1) • AP (AWS ap-southeast-2)
		CAN Region • WD10 (AWS ca-central-1) • AP (AWS ca-central-1)

Architecture

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 is a key feature of the Workday service. Multi-tenancy enables multiple Customers to share one physical instance of the Workday system while isolating each Customer's application data to their tenant.

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. End-user access utilizes role-based security logic to authenticate the user and to ensure they have been granted a role that allows the transaction.

Within a tenant, Workday facilitates the examination of transaction audits. Workday Core's distinctive architecture, notably the Object Management System (OMS), allows for data auditing. Every user-made modification is documented, including the old and new values, the user's identity, and a timestamp. Auditing tools and procedures are integrated into the system's core, capitalizing on the immutable nature of the object model. Non-destructive updates safeguard all historical data, facilitating a comprehensive audit trail.

Multi-tenancy

Multi-tenancy is a key feature of the Workday service. Multi-tenancy enables multiple Customers to share one physical instance of the Workday system while isolating each Customer's application data to their tenant.

Within a tenant, Workday facilitates the examination of transaction audits. Workday Core's distinctive architecture, notably the Object Management System (OMS), allows for data auditing. Every user-made modification is documented, including the old and new values, the user's identity, and a timestamp. Auditing tools and procedures are integrated into the system's core, capitalizing on the immutable nature of the object model. Non-destructive updates safeguard all historical data, facilitating a comprehensive audit trail.

Hosting Environments

The Workday application and Customer tenants are hosted in co-location data center facilities and/or 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) or Google Cloud Platform (GCP). Portions of Workday Extend, Media Cloud, 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 Workday's public cloud service providers.

Adaptive Planning (AP) customer instances are hosted on AWS.

Sub-service Organizations and Complementary Subservice Organization Controls (CSOCs)

AWS and GCP are 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 and GCP 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 organizations:

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.	User access to the internal Amazon network is not provisioned unless an active record is created in the HR System by Human Resources, Access is automatically provisioned with least privilege per job function. First time passwords are set to a unique value and changed immediately after first use.
	IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.
	IT access privileges are reviewed on a periodic basis by appropriate personnel.
	User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
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.
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.
	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
	Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
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.

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	Monitoring and alarming are configured by Service Owners to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics.
	Incidents are logged within a ticketing system, assigned a severity rating and tracked to resolution.
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 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.
	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.

Sub-service Organization – Amazon Web Services (AWS)	
Criteria	**Control**
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.
Sub-service Organization – Google Cloud Platform (GCP)	
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.	Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
	Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, secondary identification mechanisms, and/or physical locks.
	Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
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.	Critical power and telecommunications equipment in data centers is physically protected from disruption and damage.
	Redundant power is utilized to support the continued operation of critical data center equipment in the event of a loss of the primary power source(s).
	Data centers are equipped with fire detection alarms and protection equipment.
	Critical data center equipment supporting products and services are continuously monitored and subject to routine preventative and regular maintenance processes (including ad-hoc repairs) in accordance with organizational requirements.

Sub-service Organization – Google Cloud Platform (GCP)	
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.	Logical access to organization owned network devices is authenticated via user ID, password, security key, and/or certificate.
	Logical access to network devices is restricted to authorized personnel and is periodically reviewed.
	Only users with a valid user certificate, corresponding private key and appropriate authorization (per host) can access production machines via SSH.
	The organization maintains formal user registration and de-registration procedures for granting and revoking access.
	The organization has an established policy specifying that access to information resources, including data and the systems which store or process data, is authorized based on the principle of least privilege.
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.	Changes to network configurations are reviewed and approved prior to deployment.
	Changes to the organization's systems are tested before being deployed.
	System changes are reviewed and approved by a separate technical resource before moving into production.
CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The organization has an established incident response policy that is reviewed on a periodic basis and outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents which are categorized by severity
	The organization maintains a framework that defines how to organize a response to security and privacy incidents.
	Information security incidents are documented per the organization's Incident Response Policy. Information from these events is used to prevent future incidents and can be used as examples for information security training.
	The organization has established a dedicated security team engaging in security and privacy of customer data and managing security 24 x 7 worldwide.
	The organization maintains policies and procedures regarding the notification of data breaches, in accordance with applicable laws.

Sub-service Organization – Google Cloud Platform (GCP)	
Criteria	**Control**
CC7.3 (cont'd)	The organization provides external users with mechanisms to report security issues, incidents and concerns
PI1.2: The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.	The organization's information processing resources are distributed across distinct, geographically dispersed processing facilities to support service redundancy, and availability.
	Customer data that is uploaded or created is encrypted at rest.
	Integrity checks are in place at the application level to ensure data integrity.

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, Privacy and Responsible Artificial Intelligence (AI) training.
- 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 continuously tracking and analyzing the service availability for all customers within our production data center environments. Service availability metrics are reviewed by management on a regular basis, typically quarterly. This process involves:

- Monthly Aggregation and SLA Comparison: Workday Core Customer availability data is aggregated monthly and compared against contractually-defined Service Level Agreements (SLAs) to ensure compliance.

- Monthly Qualitative Review: A monthly qualitative review is conducted, incorporating insights from activities that could potentially impact service availability.

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. Risk is determined based on the classification of data being handled by the third party, as well as an assessment of the supplier's security controls. 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.

Workday maintains privacy and confidentiality practices in accordance with contractual obligations.

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. Workday defines key security and operational roles and responsibilities as follows:

- **Senior Management Team** – Workday has established a Senior Management Team consisting of cross-functional leadership. The Senior Management Team meets monthly to discuss strategic direction, major initiatives, and ensure alignment across all organizational leaders.

- **Chief Information Officer (CIO)** – Oversees the company's global Business Technology (BT) 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 Information Security Officer (CISO)** – 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 CISO is also responsible for ensuring that security risks are communicated.

- **Head of Privacy** - Responsible for helping the Company adhere to applicable global data protection laws, regulations, contractual commitments and privacy and compliance requirements.

- **Compliance and Integrity Team** - Responsible for promoting a culture guided by integrity and compliance and providing clear guidelines for decision-making and ethical conduct.

- **Chief Responsible AI Officer –** Responsible for the development and implementation of Workday's Responsible AI Governance Program that identifies sensitive AI use cases and provides detailed guidance and guardrails for the development of AI products and technologies.

- **Internal Audit** – Responsible for providing an independent and objective assessment of the Company's internal risk management program and internal controls frameworks to validate that the Company is operating effectively and as designed.

- **Cybersecurity Governance, Risk, and Compliance, (cGRC)** – Responsible for the strategy and execution of Workday's cybersecurity culture and vigilance across the enterprise through policy & standards governance, risk detection, evaluation, & mitigation, and third party independent audit reports and certifications (e.g., SOC, ISO), as well as building & maintaining customer trust through representation of Workday's security & privacy practices.

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

- **Change and Release Enablement** – Responsible for overseeing the software change management process and communicating milestones and status updates related to upcoming releases.

- **Infrastructure and Production Engineering** – 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.

- **Customer Support** – Responsible for responding to and collaborating with Customers when they believe that the Service is not operating as designed.

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.

In order to provide the basis for Management's Assertion on the design and operating effectiveness of the controls to achieve the related criteria, periodic inquiry of each control owner and/or operator is performed and documentation provided is reviewed by management which support the achievement of each criteria.

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.

Upon hire, every new employee signs a Proprietary Information and Inventions Agreement (PIIA) or equivalent, detailing company practices and procedures in place that are designed to promote and maintain the integrity of operations.

A set of principles and guidelines are made available to all employees to enable, develop, and encourage connections with management for alignment of employee qualifications and performance with Workday's business objectives to support the achievement of the Company's goals.

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 ISO 27001 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 criteria 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. This includes an annual assessment by the Internal Audit team to evaluate the design and operating effectiveness for controls identified within the risk assessment, and ensure corrective actions are taken as necessary. The controls assessment is completed over a span of three years with a sample of ISMS/PIMS controls tested every year. Additionally, the Internal Audit team is also assessed by an external auditor as part of the certification of the ISMS to the ISO 27001 Standard.

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.

Monitoring

Workday has designated teams responsible for monitoring the backup schedule and status of backup jobs. If a backup job fails, the status is reflected in dashboard tooling, and the backup is regenerated to resolve the issue. If the issue persists, the team will work to resolve the issue until it is fixed. Corrective action and root cause analysis is documented in the issue ticket.