



---

## System and Organization Controls 3 Report

Management's Report of its Assertions on the Effectiveness of Its Controls over the Workday Peakon Employee Voice System Based on the Trust Services Criteria for Security and Availability

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 Peakon Employee Voice System Based on the Trust Services Criteria for Security and Availability**

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

- Identifying the Workday Peakon Employee Voice (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 service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Workday Peakon Employee Voice (System) to mitigate risks that threaten the achievement of the service commitments and system requirements
- Selecting the trust services categories that are the basis of our assertion

Workday, Inc. uses Amazon Web Services (AWS) to provide infrastructure-as-a-service (IaaS) services. The boundaries of the System presented in Attachment A includes only the controls of Workday, Inc. and excludes controls of AWS. However, the description of the boundaries of the system does present the types of controls Workday, Inc. assumes have been implemented, suitably designed, and operating effectively at AWS. Certain trust services criteria can be met only if AWS' controls assumed in the design of Workday, Inc.'s controls are suitably designed and operating effectively along with the related controls at Workday, Inc. 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, 2022 to September 30, 2023, to provide reasonable assurance that the service commitments and system requirements were achieved based on the criteria relevant to security and availability set forth in the AICPA's TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, if the Subservice Organizations applied the controls assumed in the design of Workday's controls throughout the period October 1, 2022 to September 30, 2023.

**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 Peakon Employee Voice System Based on the Trust Services Criteria for Security and Availability (Assertion), that Workday, Inc.'s controls over the Workday Peakon Employee Voice system (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 criteria relevant to security and availability (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, Inc. uses Amazon Web Services (AWS) (Subservice Organization) to provide infrastructure-as-a-service (IaaS) services. The Description of the boundaries of the System (Attachment A) indicates that Workday, Inc.'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' controls, assumed in the design of Workday, Inc.'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, Inc.'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, 2022 to September 30, 2023.

### **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 its service commitments and system requirements and the risks that would threaten the achievement of its service commitments and service requirements that are the objectives of the 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

### **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.

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 and have applied the AICPA's Statement on Quality Control Standards.

#### ***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 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 if the Subservice Organization controls assumed in the design of Workday's controls operated effectively throughout the period October 1, 2022 to September 30, 2023.

A handwritten signature in black ink that reads 'Ernst &amp; Young LLP'.

February 13, 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. 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’s top priority is keeping Customer Data/Customer Content secure. Workday employs security measures at the organization, architectural, and operational levels to ensure that Customer Data/Customer Content, applications, and infrastructure remain safe.

#### **Workday Peakon Employee Voice Overview**

Workday Peakon Employee Voice is an employee success platform that enables HR leaders and managers to have data-driven discussions that go beyond the HR team, and better understand the return from investments in employee experience. The Workday Peakon Employee Voice platform identifies the relationship between employee engagement with business metrics, helps users understand how various drivers of engagement affect other areas of their business, and runs simple, user-friendly, and non-mathematical queries to support board-level decision making.

#### **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 the Workday Peakon Employee Voice application. Multi-tenancy enables multiple Customers to share one physical instance of the Workday Peakon Employee Voice system while isolating each tenant’s (Customer’s) application data. This is supported via logically separating all customer data at the database level using unique keys and table relationships.

##### **Hosting Environments**

The Workday Peakon Employee Voice service is hosted from Amazon Web Services (AWS) - eu-west-1 (Dublin, Ireland) being the primary hosting location whereas eu-central-1 (Frankfurt, Germany) is used as backup/DR region.



**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 organizations:

Sub-service Organization Controls	
Criteria	Control
<b>CC6.1:</b> 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.	AWS: Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
	AWS: Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters.
	AWS: VPC-Specific – Network communications within a VPN Gateway are isolated from network communications within other VPN Gateways.
	AWS: 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.
	AWS: 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.
<b>CC6.2:</b> 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.	AWS: IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.
	AWS: 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 Controls	
Criteria	Control
<p><b>CC6.3:</b> 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.</p>	<p>AWS: IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.</p>
	<p>AWS: User access to Amazon systems is revoked within 24 hours of the employee record being terminated (deactivated) in the HR System by Human Resources.</p>
	<p>IT access privileges are reviewed on a periodic basis by appropriate personnel.</p>
<p><b>CC6.4:</b> 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.</p>	<p>AWS: Physical access to data centers is approved by an authorized individual.</p>
	<p>AWS: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.</p>
<p><b>CC6.5:</b> 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.</p>	<p>AWS: All AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones.</p>
<p><b>CC7.1:</b> 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.</p>	<p>AWS: AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.</p>
<p><b>CC8.1:</b> The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.</p>	<p>AWS: 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.</p>



Sub-service Organization Controls	
Criteria	Control
<p><b>A1.2:</b> 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.</p>	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.
	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.
<p><b>A1.3:</b> The entity tests recovery plan procedures supporting system recovery to meet its objectives.</p>	AWS: When disk corruption or device failure is detected, the system automatically attempts to restore normal levels of object storage redundancy.
	AWS: Objects are stored redundantly across multiple fault-isolated facilities.
	AWS: The design of systems is sufficiently redundant to sustain the loss of a data center facility without interruption to the service.
	AWS: 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 the Workday Peakon Employee Voice service. 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 Peakon Employee Voice application, and the financial, system, operational and compliance requirements that Workday has established for the services.

Workday makes certain Availability 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 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 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 the Workday Peakon Employee Voice application.



---

## **C. AVAILABILITY**

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.

Workday's availability commitments are communicated in each Customer's MSA. Workday's availability service level agreement is posted on the Workday Community website.

A process for Customers and external users to inform the Company of system availability issues is posted on the Workday Community website. The process outlines steps for a Customer's Named Support Contact to follow to troubleshoot availability issues, as well as the process to open a Support Case if the availability issue persists.

## **D. SECURITY PROGRAM**

Workday maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data/customer content, protect against security threats or data breaches, and prevent unauthorized access to our customers' data.

## **E. 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 superior 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 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 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 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.

Workday regularly posts information on the Workday Community website.

### **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.