System and Organization Controls 3 Report

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

For the Period October 1, 2021 to September 30, 2022

Management's Report of its Assertions on the Effectiveness of Its Controls over the Workday Peakon Employee Voice 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 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) and Heroku (Subservice Organizations) to provide infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services respectively. The boundaries of the System presented in Attachment A includes only the controls of Workday and excludes controls of AWS and Heroku, however the description of the boundaries of the system does present the types of controls Workday assumes have been implemented, suitably designed, and operating effectively at AWS and Heroku. Certain trust services criteria can be met only if AWS and Heroku's controls assumed in the design of Workday's controls are suitably designed and operating effectively along with the related controls at Workday. However, we perform annual due diligence procedures for third-party sub-service providers and based on the procedures performed, nothing has been identified that prevents us from achieving our specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period October 1, 2021 to September 30, 2022, 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, 2021 to September 30, 2022.

Workday, Inc.

Proprietary Information, All Rights Reserved 2022 by 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 Based on the Trust Services Criteria for Security and Availability (Assertion), that Workday's controls over the Workday Peakon Employee Voice (System) were effective throughout the period October 1, 2021 to September 30, 2022, 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) and Heroku Services (Heroku) to provide infrastructure-as-a-service (IaaS) and platform-as-a-service (PaaS) services respectively. The Description of the boundaries of the System (Attachment A) indicates that Workday's controls can provide reasonable assurance that certain service commitments and system requirements, based on the applicable trust services criteria, can be achieved only if AWS and Heroku's controls, assumed in the design of Workday's controls, are suitably designed and operating effectively along with related controls at the service organization. The description of the boundaries of the system presents Workday's system and the types of controls that the service organization assumes have been implemented, suitably designed, and operating effectively at AWS and Heroku. Our examination did not extend to the services provided by AWS and Heroku, and we have not evaluated whether the controls management assumes have been implemented at AWS and Heroku have been implemented or whether such controls were suitably designed and operating effectively throughout the period October 1, 2021 to September 30, 2022.

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 the 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 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 requirement

Our responsibilities

Our responsibility is to express an opinion on the Assertion, based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Workday's relevant security and availability

Building a better working world

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 AICAP'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's controls over the System were effective throughout the period October 1, 2021 to September 30, 2022, to provide reasonable assurance that its service commitments and system requirements were achieved based on the applicable trust services criteria if the Subservice Organizations controls assumed in the design of Workday's controls operated effectively throughout the period October 1, 2021 to September 30, 2022.

Ernst & Young LLP

December 21, 2022

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 secure. Workday employs security measures at the organization, architectural, and operational levels to ensure that Customer Data, 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 in Amazon Web Services (AWS) and Heroku.

Heroku was in scope only for the period from October 1, 2021 to January 25, 2022, prior to its decommission.

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

AWS and Heroku (hosted on AWS) are responsible for operating, managing, and controlling various components of the virtualization layer and storage as well as the physical security and environmental

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

controls of these environments. Controls operated by AWS and Heroku are not included in the scope of this report.

The affected control 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**
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.	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.
	Heroku: Appropriate identifications and authentication are required to perform actions on the production infrastructure.
	Heroku: Security groups are configured to restrict access to the Heroku network.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

Sub-service Organization Controls	
Criteria	**Control**
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.	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.
	Heroku: Appropriate identifications and authentication are required to perform actions on the production infrastructure.
	Heroku: Account creation and modifications are authorized by management and documented or are granted by default based on the users' role per configurations in the access management system.
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.	AWS: IT access above least privileged, including administrator access, 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.
	IT access privileges are reviewed on a periodic basis by appropriate personnel.
	Heroku: Account creation and modifications are authorized by management and documented or are granted by default based on the users' role per configurations in the access management system.
	Heroku: Production access is revoked in a timely manner upon termination.
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.	AWS: Physical access to data centers is approved by an authorized individual.
	AWS: Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

Sub-service Organization Controls	
Criteria	**Control**
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.	AWS: 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: AWS performs external vulnerability assessments at least quarterly, identified issues are investigated and tracked to resolution in a timely manner.
	Heroku: Current and prior configurations for production servers, network devices, and databases are maintained in a version management system.
	Heroku: Emergency changes are performed in accordance with Heroku's change management procedure.
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: 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.
	Heroku: Secure encryption algorithms are used to remotely manage production infrastructure.
	Heroku: Changes to application and infrastructure components for Heroku are subject to peer review and/or approval by management, and testing.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

Sub-service Organization Controls	
Criteria	**Control**
A1.2: The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Amazon-owned data centers are protected by fire detection and suppression systems.
	Amazon-owned data centers are air-conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon-owner data centers.
	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
	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.
	Heroku: Primary and secondary storage/processing sites are separated. Data is directly replicated between sites.
	Heroku: Backups are performed and retained in accordance with the defined schedule in the Backup and Recovery process.
	Heroku: Backups are monitored on a periodic basis for success and failure. Failures are investigated and resolved in a timely manner.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

Sub-service Organization Controls	
Criteria	**Control**
A1.3: The entity tests recovery plan procedures supporting system recovery to meet its objectives.	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.
	Heroku: The platform is configured for high availability across multiple availability zones.
	Heroku: The disaster recover activities are reviewed and tested annually against the established Recovery Time Objective (RTO).

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 Peakon application, and the financial, system, operational and compliance requirements that Workday has established for the services.

Workday makes certain Security and Availability 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. 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.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

- 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 and Processing Integrity

Workday monitors health, performance, and reliability of the production environment via monitoring tools on a 24 x 7 basis. Any critical issues or anomalies identified are escalated and actively worked to resolution. 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 third parties, Workday obtains assurance through a report or certification on the effectiveness of the control environment documented by the outsourced provider's independent auditor. Each report or certification is reviewed on an annual basis by the Technology Compliance team, and reviews are documented using an internal tracking system. Security and privacy considerations are evaluated during the vendor contracting process. Any issues identified are evaluated based on risk and potential impact to the Company and its Customers.

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

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

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 the Privacy and Compliance teams helps ensure products and releases adhere to applicable laws and requirements as well as internal documented policies and procedures. All major application releases are approved by the Chief Privacy Officer before moving to production, representing that Workday develops and designs its Service in conjunction with established Privacy by Design and Privacy by Default principles.

Security Program

Workday maintains a formal and comprehensive security program designed to ensure the security and integrity of customer data, protect against security threats or data breaches, and prevent unauthorized access to our customers' 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 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 relevant industry risks are periodically assessed and reviewed by Workday senior management. Company policies and procedures focused on risk management within the company, as well as acceptable usage and other security related areas of focus, are maintained, updated, and communicated to employees on a regular basis. These policies and procedures are also available to Workday employees on the company intranet.

On an annual basis, a formal risk assessment is performed by the Privacy and Technology Compliance teams as part of the ISO27001 Information Security Management System (ISMS) requirements. The risk assessment is performed by using the Workday ISO27001 risk assessment as a basis for risk identification, with additional risks that threaten the achievement of the control objectives added as appropriate. As

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.

part of this process, threats to security, confidentiality, availability, and integrity of Customer Data and threats to the privacy and protection of personal data provided as Customer Data are identified and the risks from these threats are formally assessed.

Based on the risk assessment, program changes are made, as necessary, and the Privacy and Technology Compliance teams monitor the effectiveness of the associated programs, including the Privacy program

Information and Communication

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

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

The Company regularly posts information about product enhancements on Workday Community. Workday Community contains information to assist Customers with the Workday Peakon Employee Voice application. The content is searchable, and includes the following:

Monitoring

Operations teams are responsible for monitoring the effectiveness of internal controls in the normal course of operations. Deviations in the operation of internal controls, including major security, availability, and processing integrity events are reported to senior management. In addition, any Customer issues are communicated to the appropriate personnel using a web-based issue tracking tool.

Proprietary Information, All Rights Reserved 2022 by Workday, Inc.