Ernst & Young LLP
Suite 1600
560 Mission Street
San Francisco, CA
94104-2907

Tel: +1 415 894 8000
Fax: + 415 894 8099

Report of Independent Accountants

Management of Workday, Inc.

We have examined management's assertion that Workday, Inc., during the period November 1, 2015 through September 30, 2016, maintained effective controls to provide reasonable assurance that:

- the Workday Enterprise Cloud Applications System was protected against unauthorized access, use, or modification
- the Workday Enterprise Cloud Applications System was available for operation and use, as committed or agreed
- the Workday Enterprise Cloud Applications System processing is complete, valid, accurate, timely, and authorized
- information within the Workday Enterprise Cloud Applications System designated as confidential is protected as committed or agreed
- personal information within the Workday Enterprise Cloud Applications System was collected, used, disclosed, and retained as committed or agreed

based on the criteria for security, availability, processing integrity, confidentiality, and privacy in the American Institute of Certified Public Accountants' TSP Section 100A, Trust Services Principles and Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy. This assertion is the responsibility of Workday, Inc.'s management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and, accordingly, included (1) obtaining an understanding of Workday, Inc.'s relevant security, availability, processing integrity, confidentiality, and privacy controls, (2) testing and evaluating the operating effectiveness of the controls and (3) performing such other procedures as we considered necessary in the circumstances. We believe that our examination provides a reasonable basis for our opinion.

Because of inherent limitations in controls, error or fraud may occur and not be detected. Furthermore, the projection of any conclusions, based on our findings, to future periods is subject to the risk that the validity of such conclusions may be altered because of changes made to the system or controls, the failure to make needed changes to the system or controls or a deterioration in the degree of effectiveness of the controls.

In our opinion, Workday, Inc.'s management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, processing integrity, confidentiality, and privacy.

Ernst & Young LLP

January 20, 2017

Report of Management on the System and Controls Over the Workday Enterprise Cloud Applications System Based on the Trust Services™ Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy

Workday Inc. maintained effective controls over the security, availability, processing integrity, confidentiality, and privacy of its Workday Enterprise Cloud Applications System to provide reasonable assurance that:

- The Workday Enterprise Cloud Applications System was protected against unauthorized access, use, or modification
- The Workday Enterprise Cloud Applications System was available for operation and use as committed or agreed
- The Workday Enterprise Cloud Applications System processing was complete, valid, accurate, timely, and authorized
- Information within the Workday Enterprise Cloud Applications System designated as confidential was protected as committed or agreed
- Personal information within the Workday Enterprise Cloud Applications System was collected, used, disclosed, and retained as committed or agreed

during the period November 1, 2015 through September 30, 2016, based on the criteria for the Security, Availability, Processing Integrity, Confidentiality, and Privacy principles set forth in the American Institute of Certified Public Accountants (AICPA) TSP section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

The included System Description identifies the aspects of the Workday Enterprise Cloud Applications System covered by our assertion.

Barbara Cosgrove
Chief Privacy Officer

System Description of Workday's Enterprise Cloud Applications

Corporate Overview

Workday, headquartered in Pleasanton, California, is a provider of enterprise cloud applications for human resources and finance. Founded by PeopleSoft veterans David Duffield and Aneel Bhusri, Workday delivers human capital management, financial management, and analytics applications designed for the world's largest organizations.

Customers

Workday customers represent a range of industries, sizes and requirements – from mid-size companies looking to replace paper-based, manual processes to larger enterprises looking for a modern replacement to on premise enterprise resource planning (ERP) systems. Hundreds of companies, ranging from medium-sized businesses to Fortune 50 enterprises, have selected Workday.

Enterprise Cloud Applications

Workday provides Enterprise Cloud Applications for:

Human Capital Management (HCM) – Workday human resource and talent management applications that help organizations recruit, manage, train, organize, staff, pay, and develop a global workforce of both employees and contingent workers through the hire-to-retire process.

Financial Management – Applications that manage an organization's financial accounting, reporting and management of information necessary to operate and measure the organization. In addition, these applications support the planning, budgeting, order-to-cash, revenue management, procure-to-pay, and expense management processes.

Payroll Solutions – Allows customers to group employees, manage payroll calculation rules, and pay employees according to their organizational, policy and reporting needs.

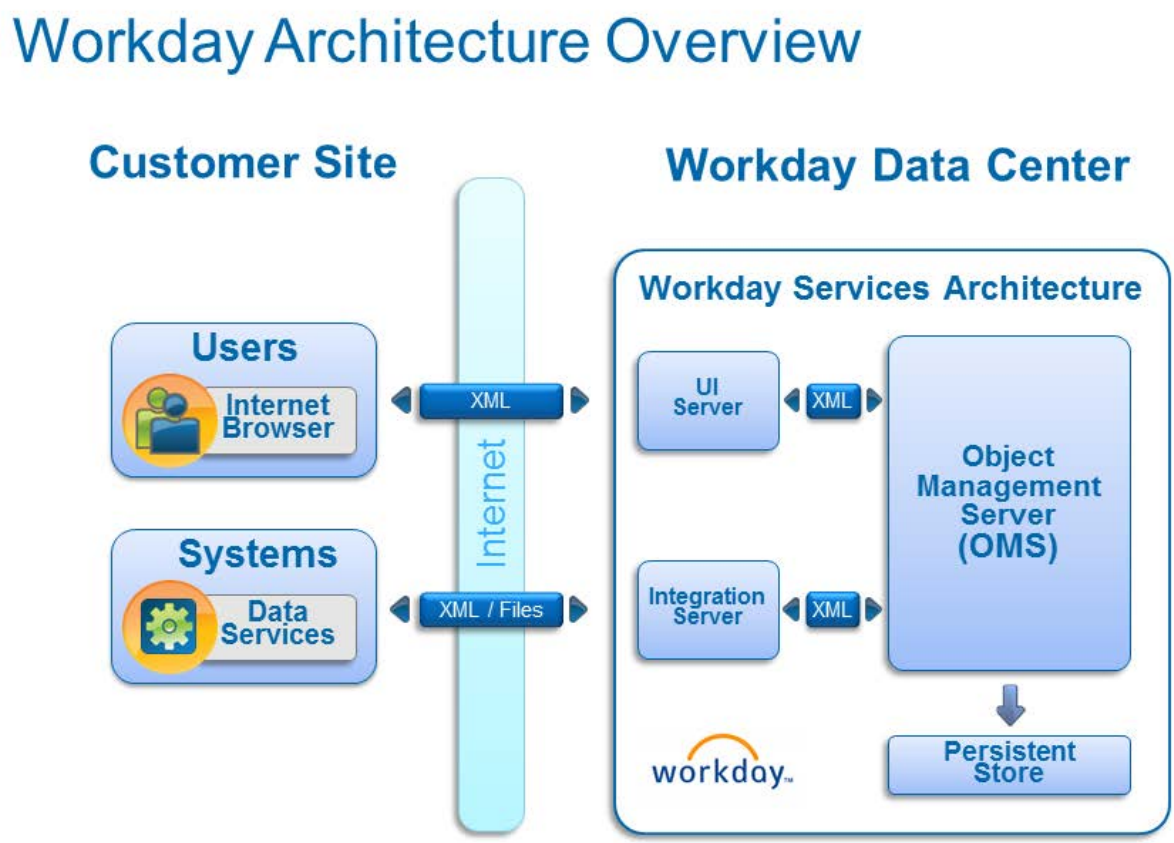
Student – Higher education-focused applications – both delivered and being designed – that manage the student and faculty lifecycle, including student recruiting, admissions, curriculum management, records, academic advising, financial aid, and student financials.

Insights Foundation – Insights Foundation is an analytics platform for combining Workday data with data from multiple non-Workday data sources of various types, sizes or volume to provide business insight.

Infrastructure

Workday uses a tiered architecture, including proprietary applications supported by UI/integration servers, application servers, and database servers. Workday also utilizes various automated systems to monitor the security, availability and performance of Workday services.

Technology



Software as a Service (SaaS) – Workday delivers applications via a software as a service (SaaS) model. In this service delivery model, Workday is responsible for providing the infrastructure (i.e. hardware and middleware that comprise the Workday infrastructure), data security, software development (i.e. software updates and patches), and operational processes (i.e. operation and management of the infrastructure and systems to support the service).

Workday Private Cloud (WPC) – Workday Private Cloud (WPC) is the next generation of Workday infrastructure – virtualized servers running Workday services that provide for scalability and flexibility of resources. A select group of User Interface (UI) and Integration servers within a single data center have been migrated to the WPC architecture. WPC fully exists within Workday's data center infrastructure and is included within the scope of this report.

Multi-tenancy – Multi-tenancy is a key feature of Workday. Multi-tenancy enables multiple customers to share one physical instance of the Workday system while isolating each tenant's (customer's) application data. Workday accomplishes this through the Workday Object Management Server (OMS). Every user ID is associated with exactly one tenant, which is then used to access the Workday application. All instances of application objects (such as Organization, Worker, etc.) are tenant-based, so every time a new object is created, that object is also irrevocably linked to the user's tenant. The Workday system maintains these links automatically, and restricts access to every object based on the user ID. The Workday system restricts access to objects based on the user ID and tenant.

Compliance – Compliance, privacy, and security considerations are core to the overall design of Workday. Workday's privacy by design philosophy underlies many privacy-enhancing features. New features are evaluated early in the development stage and throughout the entire development processes to assess and address potential privacy and compliance impacts. In addition, Workday employs a unified approach to security at all computing layers. Access for end users to view or modify data within the application is only granted using a designated end point (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 end users.

Access through the operating system and designated endpoint utilizes role-based security logic to authenticate the user and to make sure they have been granted a role that allows the update.

Workday provides non-destructive data updates for a complete audit trail of changes made to application data in the Company's solution. When any update is made, the system records the user who made the change and the time they made the change. Reports showing system update activity by user for selected time periods are delivered with all Workday applications.

Customer Data

Workday defines Customer Data as the electronic data or information submitted by the Customer to the Workday system. Customer Data is deemed confidential. Access to Customer Data is tightly restricted to authorized personnel through the use of physical and logical access controls.

The Customer determines what data is entered into the Workday applications and configures the appropriate security for the data, including who can access and use the data. Additionally, where applicable, the customer manages any notification or consent requirements, and maintains the accuracy of the data. Workday then processes the data in accordance with its contractual agreement with the customer.

Business Process Framework

Workday's embedded Business Process Framework allows companies to customize Workday to meet each organization's unique business requirements via configurable business processes that require no coding.

With the Workday Business Process Framework, companies can:

- Configure, manage, and optimize business processes to ensure consistency or address specific needs across different organizations
- Deploy processes quickly by starting from a catalog of pre-defined business processes
- Reconfigure business processes as business needs evolve. Add or remove steps from an established business process without writing any code. Apply a process to an entire enterprise or configure processes to meet the needs of specific organizations within an enterprise.
- Establish control, visibility, and compliance through the ability to monitor and audit all process and transaction statuses
- Use pre-defined workflow processes. Workday delivers over 400 pre-defined business process definitions to help accelerate implementations and provide a starting point for additional configuration.
- Maintain rules, roles, routings, and policy documents. Business rules, approval paths, roles, and document attachments all help ensure proper routing and review in each step of a business process.

- Utilize Workday Organization Management. Any adjustments to organization structures take effect in real time, with changes to roles and reporting structures incorporated instantly into all defined business processes and workflows.

Customer Responsibilities

Customers are responsible for establishing, monitoring and maintaining sufficient internal controls to ensure integrity and protection of information entered into Workday's Enterprise Cloud Applications. Customers are similarly responsible for establishing, monitoring and maintaining sufficient internal controls to ensure that collection, processing and sharing of information entered into Workday's Enterprise Cloud Applications is in accordance with regulations or laws applicable to the customer. Customers are also responsible for monitoring and testing Workday Service Updates and Feature Releases, including integration processing. Customers should communicate issues encountered to Workday.

People

Workday management is responsible for directing and controlling operations, as well as establishing, communicating, and monitoring company-wide control 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:

- **Chief Privacy Officer (CPO)** – Responsible for promoting a culture of integrity and ethical behavior and helping Workday adhere to applicable laws, regulations, contractual commitments and privacy compliance requirements.
- **Chief Security Officer (CSO)** – Oversight to management related to the identification and evaluation of security vulnerabilities involved in Workday's technology and operations. Security incident planning and management is also a key focus of the Chief Security Officer.
- **Development Team** – Responsible for the consistent promotion and development of security features within the Workday applications.
- **Program Management Office (PMO)** – The Company's Program Management Office is responsible for overseeing the software change management process, and holds weekly meetings to communicate milestones and internal status related to upcoming releases.
- **Quality Assurance** – Responsible for manual and automated testing to ensure the quality of software.
- **Security Council** – Workday has established a Security Council consisting of cross-functional management representatives that is chaired by the Chief Security Officer. The Security Council meets on a monthly basis to assess the direction and visibility of management support for security initiatives.
- **Infrastructure and Environments Operations Teams** – Responsible for the administration and monitoring of user access to Workday's internal systems, and system administration and management of application, databases, and operating system security.