Report of Independent Accountants

Board of Directors
Workday, Inc.

We have examined management’s assertion that Workday, during the period July 1, 2013 through December 31, 2013,

- maintained effective controls:
  - to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System was available for operation and use, as committed and agreed; and
  - to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System information designated as confidential was protected as committed or agreed; and
  - over the privacy of personal information collected in its Workday Cloud-based Enterprise Applications to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice; and
  - to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System was protected against unauthorized access (both physical and logical)

based on the 2009 version of the AICPA/CICA Trust Services Availability, Confidentiality, Privacy, and Security Criteria issued by the American Institute of Certified Public Accountants (AICPA) and CPA Canada, that includes Generally Accepted Privacy Principles.

- Complied with its commitments in its privacy notice, which is dated December 20, 2013 and is available at http://www.workday.com/company/privacy.php:

This assertion is the responsibility of Workday 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’s relevant availability, confidentiality, privacy, and security controls, (2) testing and evaluating the operating effectiveness of the controls; (3) testing compliance with Workday’s commitments in its privacy notice and (4) 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 the nature and inherent limitations of controls, Workday’s ability to meet the aforementioned criteria and the commitments in its privacy notice may be affected. For example, fraud, unauthorized access to systems and information and failure to comply with internal and external policies or requirements may not be prevented or detected. Also, 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’s management’s assertion referred to above is fairly stated, in all material respects, based on the Trust Services Availability, Confidentiality, Privacy, and Security Criteria.

The SOC 3 SysTrust for Service Organizations seal on Workday’s Web site constitutes a symbolic representation of the contents of this report and it is not intended, nor should it be construed, to update this report or provide any additional assurance.

Ernst & Young LLP

March 6, 2014
Management’s Assertion Regarding the Effectiveness of Its Controls
Over the Workday Cloud-based Enterprise Applications
Based on the Trust Services™ Principles and Criteria for
Availability, Confidentiality, Privacy, and Security

March 6, 2014

Workday maintained effective controls over the availability, confidentiality, privacy, and security of its Workday Cloud-based Enterprise Applications System:

- to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System was available for operation and use, as committed and agreed; and
- to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System information designated as confidential was protected as committed or agreed; and
- over the privacy of personal information collected in its Workday Cloud-based Enterprise Applications to provide reasonable assurance that the personal information was collected, used, retained, disclosed, and disposed of in conformity with its commitments in its privacy notice; and
- to provide reasonable assurance that the Workday Cloud-based Enterprise Applications System was protected against unauthorized access (both physical and logical);

and Complied with its commitments in its privacy notice, which is dated December 20, 2013 and is available at http://www.workday.com/company/privacy.php during the period July 1, 2013 through December 31, 2013, based on the 2009 version of the Trust Services™ Availability, Confidentiality, Privacy, and Security Criteria established by the American Institute of Certified Public Accountants (AICPA) and CPA.

Our attached System Description of the Workday Cloud-based Enterprise Application System identified the aspects of the Workday Cloud-based Enterprise Applications covered by our assertion.

Barbara Cosgrove
Chief Privacy Officer
System Description of Workday's Cloud-based Enterprise Applications

Corporate Overview

Workday, headquartered in Pleasanton, California is a provider of Cloud-based Enterprise Applications. Founded by PeopleSoft veterans David Duffield and Aneel Bhusri, Workday delivers unified Human Capital Management, Payroll, and Financial Management solutions designed for today’s organizations and the way people work.

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.

Cloud-based Enterprise Applications

Workday provides Cloud-based Enterprise Applications for:

- **Human Capital Management (HCM)** – Workday Human Resource and Talent Management applications that help 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 to financial accounting and reporting, these applications support the 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.

- **Integration Cloud** – Workday Integration Cloud eases the burden of integrations through a comprehensive solution that enables customers and partners to build and deploy integrations to the Workday Cloud without the need for any on-premise middleware.

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.
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).

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 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 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 web browser 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 200 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 the propriety of access to information on Workday’s On-Demand Enterprise Business Services. Each customer should assign at least two individuals to perform security administration responsibilities. Customers are responsible for controlling the access rights and authorization limits necessary for each end user to accomplish job responsibilities. Customers are responsible for testing Workday Updates,
including integrations, in their sandbox environments before the Updates are moved to production. In addition, customers are responsible for testing changes they make to configurations, including integrations, in their sandbox before the changes are moved to production. Customers are also responsible for confirming that integrations have processed successfully by viewing the Integration Events report after an integration has been launched.

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.
- **Cloud Operations 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.