Service Organization Control 3 Report

Report on Management’s Description of System – Workday Enterprise Cloud Applications and Workday Cloud Platform Relevant to Availability, Confidentiality, Privacy, Processing Integrity, and Security

For the Period October 1, 2017 through September 30, 2018
Report of Independent Accountants

To the Management of Workday Inc.

Approach:
We have examined management’s assertion that Workday maintained effective controls to provide reasonable assurance that:

- the Workday Enterprise Cloud Applications and Workday Cloud Platform System was protected against unauthorized access, use, or modification to achieve Workday’s commitments and system requirements
- the Workday Enterprise Cloud Applications and Workday Cloud Platform System was available for operation and use to achieve Workday’s commitments and system requirements
- the Workday Enterprise Cloud Applications and Workday Cloud Platform System processing is complete, valid, accurate, timely, and authorized to achieve Workday’s commitments and system requirements
- the Workday Enterprise Cloud Applications and Workday Cloud Platform System information is collected, used, disclosed, and retained to achieve Workday’s commitments and system requirements
- personal information within the Workday Enterprise Cloud Applications and Workday Cloud Platform System is collected, used, disclosed, and retained to achieve Workday’s commitments and system requirements
during the period October 1, 2017 through September 30, 2018 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’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. 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, 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 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 and appropriate 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.

**Inherent limitations:**
There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy are achieved.

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. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

**Opinion:**
In our opinion, Workday’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.

November 30, 2018
Management’s Assertion Regarding the Effectiveness of Its Controls
Over the Workday Enterprise Cloud Applications and Workday Cloud Platform System
Based on the Trust Services Principles and Criteria for
Security, Availability, Processing Integrity, Confidentiality, and Privacy

We, as management of, Workday, Inc. ("Workday") are responsible for designing, implementing
and maintaining effective controls over the Workday Enterprise Cloud Applications and Workday
Cloud Platform System (System) to provide reasonable assurance that the commitments and
system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human
error and the circumvention of controls. Because of inherent limitations in Security controls, an
entity may achieve reasonable, but not absolute, assurance that all security events are prevented
and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations
in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their
  manufacturer or developer.
- Ineffective controls at a vendor or business partner.
- Persistent attackers with the resources to use advanced technical means and
  sophisticated social engineering techniques specifically targeting the entity.

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the
risk that controls may become inadequate because of changes in conditions or that the degree of
compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout
the period October 1, 2017 to September 30, 2018, to achieve the commitments and system
requirements related to the operation of the System using the criteria for security, availability,
processing integrity, confidentiality and privacy (Control Criteria) set forth in the AICPA's TSP
section 100A, Trust Services Principles and Criteria for Security, Availability, Processing Integrity,
Confidentiality, and Privacy. Based on this evaluation, we assert that the controls were effective
throughout the period October 1, 2017 to September 30, 2018 to provide reasonable assurance that:

- the System was protected against unauthorized access, use, or modification to achieve
  Workday’s commitments and system requirements
- the System was available for operation and use, to achieve Workday’s commitments and
  system requirements
- the System processing is complete, valid, accurate, timely, and authorized to achieve
  Workday’s commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Workday’s
  commitments and system requirements
- Personal information is collected, used, disclosed, and retained to achieve Workday’s
  commitments and system requirements
based on the Control Criteria.

Our attached description of the boundaries of the Workday Enterprise Cloud Applications and Workday Cloud Platform System identifies the aspects of the Workday Enterprise Cloud Application and Workday Cloud Platform System covered by our assertion.

Very truly yours,

Barbara M Cosgrove
Barbara Cosgrove
Chief Privacy Officer
DESCRIPTION OF THE COMPANY

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 Resources – Workday’s 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. These applications include:

- Workday Learning
- Workday Payroll
- Workday Planning (For Workforce Planning)
- Workday Recruiting
- Workday Time Tracking

Finance – Workday’s financial management applications help 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. These applications include:

- Workday Expenses
- Workday Financial Performance Management (FPM)
- Workday Grants Management
- Workday Planning (For Financial Planning)
- Workday Procurement
- Workday Projects

Analytics & Technology – Workday’s analytics and technology products include:

- Workday Benchmarking, an offering available as part of Workday Data-as-a-Service
- Workday Prism Analytics
- Workday Cloud Platform
Industry specific applications:

- Workday Inventory (For Healthcare)
- Workday Professional Services Automation (For Professional Services Organizations)
- Workday Student (for Higher Education)

Technology

Workday Architecture Overview

**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 comprised of virtualized servers running Workday services that provide enhanced scalability and flexibility of technical resources. WPC resides within Workday’s data center infrastructure.

Amazon Web Services (AWS) environments – Public Cloud and Workday Cloud Platform are included within the scope of this report.

- **Public Cloud** – Workday offers customers the option of running Workday applications in a public cloud environment hosted by Amazon Web Services (AWS), utilizing AWS Elastic Compute Cloud (EC2) and Simple Storage Service (S3). Workday applications running in this environment maintain the same level of security, change management, and logical access controls.
- **Workday Cloud Platform** – The Workday Cloud Platform enables Workday customers and partners to build extensions and applications that run on or integrate with Workday. A subset of the Cloud Platform is hosted in Amazon Web Services (AWS). The Workday-managed components of the Workday Cloud Platform utilize AWS Elastic Compute Cloud (EC2), Simple Storage Service (S3) and AWS Lambda.

Amazon Web Services 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 expected minimum controls in place at AWS.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>AWS controls expected to be in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC5.1: Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access.</td>
<td>Access to the in-scope systems requires users to authenticate using a valid unique user ID and password before being granted access.</td>
</tr>
<tr>
<td>CC5.2: New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity’s commitments and system requirements as they relate to security, availability, processing integrity, confidentiality, and privacy. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.</td>
<td>Privileged user accounts are approved by appropriate personnel prior to access being granted.</td>
</tr>
<tr>
<td>CC5.4: Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity’s commitments and system requirements as they relate to security, availability, processing integrity, confidentiality, or privacy.</td>
<td>User access is revoked within a timely manner upon notification of the employee termination event. Access privileges are reviewed on a quarterly basis by appropriate personnel.</td>
</tr>
<tr>
<td>Criteria</td>
<td>AWS controls expected to be in place</td>
</tr>
<tr>
<td>-------------------------------------------------------------------------</td>
<td>---------------------------------------------------------------------------------------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>CC5.5: Physical access to facilities housing the system (for example,</td>
<td>Only authorized personnel have access to the facilities housing the system.</td>
</tr>
<tr>
<td>data centers, backup media storage, and other sensitive locations, as</td>
<td>Badge access control systems are in place in order to access the facilities.</td>
</tr>
<tr>
<td>well as sensitive system components within those locations) is restricted</td>
<td>Visitor access to the corporate facility and data center are recorded in visitor access logs.</td>
</tr>
<tr>
<td>to authorized personnel.</td>
<td>Visitors are required to wear a visitor badge while onsite at the facilities.</td>
</tr>
<tr>
<td></td>
<td>Visitors are required to check in with security and show a government issued ID prior to being granted access the facilities.</td>
</tr>
<tr>
<td></td>
<td>Visitors are required to have an escort at all times.</td>
</tr>
<tr>
<td>CC7.4: Changes to system components are authorized, designed, developed,</td>
<td>Changes to system components are authorized, logged, tested, approved and documented.</td>
</tr>
<tr>
<td>configured, documented, tested, approved, and implemented.</td>
<td></td>
</tr>
<tr>
<td>A1.1: Current processing capacity and usage are maintained, monitored,</td>
<td>Monitoring applications are configured to monitor capacity levels and alert appropriate personnel when predefined thresholds are met.</td>
</tr>
<tr>
<td>and evaluated to manage capacity demand and to enable the implementation</td>
<td></td>
</tr>
<tr>
<td>of additional capacity to help meet the entity’s availability commitments</td>
<td></td>
</tr>
<tr>
<td>and system requirements.</td>
<td></td>
</tr>
<tr>
<td>A1.2: Environmental protections, software, data backup processes, and</td>
<td>Fire detection and suppression equipment are in place and fire extinguishers have been installed.</td>
</tr>
<tr>
<td>recovery infrastructure are authorized, designed, developed,</td>
<td>Data Centers are air conditioned to maintain appropriate atmospheric conditions. Air temperature and humidity are monitored to the appropriate levels.</td>
</tr>
<tr>
<td>implemented, operated, approved, maintained, and monitored to meet the</td>
<td>Power management equipment are in place at each facility.</td>
</tr>
<tr>
<td>entity’s availability commitments and system requirements.</td>
<td>Backup power generators are in place in case of power failure.</td>
</tr>
</tbody>
</table>

**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 Workday account 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 Workday account and tenant.
Security and Privacy – 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 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 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.

Implementation Tools

Workday provides various tools that facilitate the ease of implementing and configuring new customer tenants.

Customer Central (CC) is an optional add-on tenant for all Workday implementations that started prior to January 15th, 2018 and is a default tenant for all new implementations after January 15th, 2018. Customer Central provides Workday certified implementers access to tooling to efficiently build and maintain a customer’s non-production tenants. During the implementation engagement, Customer Central provides a centralized gateway to compare data and configuration between tenants. It facilitates the migration of Workday-delivered configuration objects from reference tenants to non-production customer tenants, as well as giving implementers the ability to migrate configuration objects between non-production tenants. Customer Central tenant is built on the same fundamental architecture as any other Customer tenant and it is hosted within Workday’s Implementation Environments and therefore, it inherits the standard security and privacy controls. Non-production customer tenants must be configured to enable interaction with the Customer Central tenant.

Object Transporter (OX) is a configuration migration tool built into customer tenants that streamline 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.

Customer Data

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

The Customer determines what data is entered into 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 and the settings implemented by the Customer.
In the normal course of operations, Customer Data exists in several environments depending on customer needs. Environments that contain Customer Data include the following:

- **Production**
  - Production – Environment for the production Workday applications

- **Non-Production**
  - Disaster Recovery – Backup environment available for disaster recovery
  - Implementation (Deployment) – Environment in use for longer-term configuration changes and testing
  - Sandbox – Environment used for testing configuration changes and training
  - Conversion Test – Environments for verification testing for Production customers
  - Advanced Conversion Test – Opt-in, non-customer facing environment for advanced testing

- **Performance/Verification**
  - Performance – Opt-in non-customer facing environment used for replication of performance issues
  - Secure Verification Environment – Opt-in, non-customer facing environment used for replication of performance issues

Any software, data, text, audio, video, images or any other content from any source that the Customer submits as part of a learning campaign within the Workday Learning Service is not in-scope for this report.

**Workday Privacy Practices**

- Workday accesses Customer Data, in accordance with the relevant agreement between customer and Workday.
- Workday processes Customer Data under the direction of its customers, and has no direct control or ownership of the personal data it processes.
- Workday retains Customer Data according to the timeframes set forth in the relevant agreement with its customers.
- 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 Data.
- Workday designs its applications to allow customers to achieve differentiated configurations, enforce user access controls, and manage data categories that may be populated and/or made accessible on a country-by-country basis.
- If required, customers are responsible for providing notice to the individuals whose data will be collected and used within the Workday application. Workday is not responsible for providing such notice to or obtaining consent from these individuals, and is only responsible for communicating its Privacy practices to Workday’s customers, which are included in formal agreements with the customers.
- Workday has appointed a Chief Privacy Officer responsible for overseeing the implementation of the privacy program in the organization.
Security Program

The following table illustrates the security program components and related policies, procedures, processes, and/or control in place to address the component.

<table>
<thead>
<tr>
<th>Security Program Components</th>
<th>Relevant Policies, Procedures, Processes, and/or Controls</th>
</tr>
</thead>
</table>
| Risk assessment and treatment | Information Security Management System (ISMS) Policy  
Risk Assessment Methodology (includes Risk Treatment Plan) |
| Security policy | Workday Service Privacy Policy  
Information Security Management System (ISMS) Policy  
Acceptable Encryption Policy  
Workday Service Privacy Policy |
| Organization of information security | Information Security Management System (ISMS) Policy  
Information Security Management System (ISMS) Handbook¹ |
| Asset management | Information Systems Configuration and Management Policy  
Acceptable Use Policy  
Mobile Device Policy |
| Human resources security | Privacy and Security Training policy  
Employment Background Check Policy  
Proprietary Information and Inventions Agreement¹  
Job Profile Summaries¹ |
| Physical and environmental security | Physical Security – Hosting Facilities Policy |
| Access control | Logical Access to Workday Systems Policy  
Password Policy  
Remote Access Policy  
Digital Key Management Policy |
| Information systems acquisition, development, and maintenance | Change Management Policies  
Change Management Process Document¹  
Handling Professional Services Data During Implementations Policy  
Access to Customer Data Policy  
Development/Product Management Access to Customer Data Policy |
| Information security incident management | Security Incident Policy  
Incident Response Plan |
| Availability and Capacity Management | Database Backup Management Policy  
Disaster Recovery Process  
Capacity Management Process and Procedures  
Operations Availability Metrics Process |
| Compliance | Employee Conduct and Discipline Guidelines¹ |

¹ This document is not a formal policy document per company guidelines that requires formal review sign-offs, however the document is available to company personnel on the company intranet.
RELEVANT ASPECTS OF INTERNAL CONTROL

As defined by the Committee of Sponsoring Organizations of the Treadway Commission (COSO), internal control is a process affected by an entity’s board of directors, management, and other personnel and consists of five interrelated components:

- **Control Environment** – Sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure.

- **Risk Management** – The entity’s identification and analysis of relevant risks to achievement of its objectives, forming a basis for determining how the risks should be managed.

- **Information and Communication** – Surrounding these activities are information and communication systems. These enable the entity’s people to capture and exchange information needed to conduct and control its operations.

- **Monitoring** – The entire process must be monitored, and modifications made as necessary. In this way, the system can react dynamically, changing as conditions warrant.

- **Control Activities** – Control policies and procedures must be established and executed to help ensure that the actions identified by management as necessary to address risks to achievement of the entity’s control objectives are effectively carried out.

Set out below is a description of the five components of internal control as it pertains to Workday that may be relevant to Customers.

**Control Environment**

**Management Controls**

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 Information Officer (CIO)** – Oversees the company’s security and global information technology (IT) organization, with responsibility for the internal deployment of Workday products as well as other innovative 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 identification and evaluation of security vulnerabilities involved in Workday’s technology and operations as well as security incident planning and management. The CISO is also responsible for ensuring that security risks are communicated.

- **Chief Privacy Officer (CPO)** – Responsible for promoting a culture of integrity and ethical behavior and helping Workday adhere to applicable global data protection laws, regulations, contractual commitments and privacy compliance requirements.
- **Development (including Product Management) and QA Team** – Responsible for the consistent promotion and development of security features within the Workday applications, as well as manual and automated testing to ensure the quality of software.

- **Program Management Office (PMO) Team** – The Company’s Program Management Office is responsible for overseeing the software change management process, and holds internal weekly meetings to communicate milestones and status updates related to upcoming releases.

- **Security Council** – Workday has established a Security Council consisting of cross-functional management representatives. The Security Council meets on a quarterly basis to assess the direction and provide management support for security initiatives.

- **Platform Infrastructure and Environments Operations Teams** – Responsible for the administration and monitoring of user access to Workday’s internal systems, administration and management of application, persistent data stores, databases, and operating system security.

- **Support Team** – Workday’s Support team is designed to respond to and collaborate with customers when they believe the Workday Services is not operating as designed.

- **Internal Audit Team** – Provides an independent and objective assessment of Workday’s internal risk management program and internal controls frameworks to validate that the Company is operating effectively and as designed.

**Personnel Policies and Procedures**

Workday employs people who are selected and valued for their intuition, intelligence, integrity and passion for delivering superior solutions to customers. The Company’s Human Resources team, Security, and Privacy, Ethics and Compliance team, together with Management, are responsible for developing, maintaining, and communicating company policies and procedures that promote Workday’s core values.

**Risk Management**

Financial, IT, 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, Ethics and Compliance team as part of the Service Organization Control reporting process. 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.

Additionally, external network, system, and application vulnerability threat assessments are performed by third party security service providers on a periodic basis. The results of these assessments are reviewed by Workday senior management, including the Chief Information Security Officer. Issues noted are assessed for criticality and severity, and assigned to the appropriate resources for remediation.

**Information and Communication**

Management is committed to maintaining effective communication with all personnel, customers and business partners. Issues or suggestions identified by Workday 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 Program Management Office 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 in the Workday Community. The Community contains information to assist Customers with Workday Enterprise Cloud Applications. The content is searchable, and the Workday Community site includes the following:

- Current Workday company and application news and events
- Relevant information to help users understand, navigate, and use the Workday system
- Link to login to the support site where customers are able to ask questions and report problems

**Monitoring**

The Infrastructure and Environments 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 prospect or customer issues are communicated to the appropriate Workday personnel using a web-based issue tracking tool. Workday employees can monitor the status of the issue tickets, and are notified when changes occur.

In order to provide the basis for Management’s Assertion on the design and operating effectiveness of controls created to achieve the related control objectives, the Privacy, Ethics and Compliance team performs inquiry of each control owner and/or operator and reviews documentation provided by management which support the achievement of each control objective.

Workday also uses automated tools and systems to monitor the security and availability of the Enterprise Cloud Applications, including network, application, database, persistent data store, and operating system activities. In addition, system and access logs are maintained for critical systems to support monitoring investigations and resolution, as necessary.

Appropriate contact with special interest groups and law enforcement authorities is maintained to support broader cybersecurity situational awareness.