Adaptive Insights, a Workday Company

System and Organization Controls 3 Report

Management’s Report of its Assertions on the Effectiveness of its Controls Over the Adaptive Insights Business Planning Cloud System Based on the Trust Services Criteria for Security, Availability, Confidentiality, and Processing Integrity

For the Period October 1, 2018 to September 30, 2019
Report of Independent Accountants

Management of Workday Inc.

Scope:
We have examined management's assertion, contained within the accompanying Management's Assertion Regarding the Effectiveness of Its Controls Over the Adaptive Insights Business Planning Cloud based on the Trust Services Criteria for Security, Availability, Confidentiality, Processing Integrity, and Privacy (Assertion), that Workday's controls over the Adaptive Insights Business Planning Cloud (System) were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that its principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, confidentiality, and privacy (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.

Management’s Responsibilities:
Workday's management is responsible for its assertion, selecting the trust services categories and associated criteria on which the its assertion is based, and having a reasonable basis for its assertion. It is also responsible for:

- Identifying the Adaptive Insights Business Planning Cloud (System) and describing the boundaries of the System.
- Identifying the principal service commitments and system requirements and the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of the system.
- Identifying, designing, implementing, operating, and monitoring effective controls over the Adaptive Insights Business Planning Cloud (System) to mitigate risks that threaten the achievement of the principal 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, 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 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:
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 principal 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 management assertion referred to above is fairly stated, in all material respects, based on the applicable trust services criteria.

January 20, 2020

We, as management of Workday are responsible for:

- Identifying the Adaptive Insights Business Planning Cloud (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 principal service commitments and service requirements that are the objectives of our system
- Identifying, designing, implementing, operating, and monitoring effective controls over the Adaptive Insights Business Planning Cloud (System) to mitigate risks that threaten the achievement of the principal service commitments and system requirement
- Selecting the trust services categories that are the basis of our assertion

Workday uses Amazon Web Services (AWS) and Dimension Data (DD) to provide infrastructure-as-a-service services, and Cyxtera as a co-location data center to provide physical security and environmental safeguards controls. The Description includes only the controls of Workday and excludes controls of AWS, DD, and Cyxtera. The Description also indicates that certain trust services criteria specified therein can be met only if AWS’s, DD’s, and Cyxtera’s controls assumed in the design of Workday’s controls are suitably designed and operating effectively along with the related controls at the Service Organization. The Description does not extend to controls of AWS, DD, and Cyxtera.

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 Workday from achieving its specified service commitments and system requirements.

We assert that the controls over the system were effective throughout the period October 1, 2018 to September 30, 2019, to provide reasonable assurance that the principal service commitments and system requirements were achieved based on the criteria relevant to security, availability, processing integrity, and confidentiality set forth in the AICPA’s TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Very truly yours,

Barbara M Cosgrove
Barbara Cosgrove
Chief Privacy Officer
ATTACHMENT A

INTRODUCTION

This section of the report, Section III, has been prepared by Workday, Inc. (“Workday” or the “Company”) management and presents an overview of the Company, including the following:

- The Adaptive Insights Business Planning Cloud provided to Customers
- Workday’s business operations primarily based in Pleasanton, California and Dublin, Ireland
- Use of Amazon Web Services (AWS) and Dimension Data (DD), as well as co-located data centers (Cyxtera) based in Santa Clara, California and Vancouver, Canada.

Section IV presents the trust services criteria that Workday should reasonably be expected to achieve on behalf of its Customers. Each trust services criteria is followed by a description of the controls in place at Workday that contribute to or otherwise affect the achievement of the applicable criteria and the Independent Service Auditor’s description of the test of controls and results. Section V contains other information provided by Workday that has not been examined by the Independent Service Auditor.

DESCRIPTION OF THE COMPANY

Corporate Overview

Workday is a provider of enterprise products for finance and human resources. Founded in 2005, Workday delivers financial management, human capital management, planning, and analytics applications designed for the world’s largest companies, educational institutions, and government agencies. Organizations ranging from medium-sized businesses to Fortune 50 enterprises have selected Workday. Workday completed its acquisition of Adaptive Insights, a cloud-based company for modernizing business planning, in August 2018.

Adaptive Insights Business Planning Cloud

The Adaptive Insights Business Planning Cloud (Adaptive Insights application) enables comprehensive planning for finance, sales, workforce, and operational planning, such as CRM, HR, and project planning.

Technology

Software as a Service (SaaS) – Adaptive Insights Business Planning Cloud offers capabilities for budgeting, reporting, consolidation, dashboards, and business intelligence that empower finance, sales, and other business leaders with insights to drive true competitive advantage. In this service delivery model, Workday is responsible for providing the infrastructure (i.e., hardware and middleware that comprise the Adaptive Insights 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 hosts the Business Planning Cloud with both co-location data centers and Infrastructure-as-a-Service providers.

Hosting Environments – Amazon Web Services (AWS) and Dimension Data (DD) are utilized as Infrastructure-as-a-Service providers hosting Adaptive Insights Business Planning Cloud. Additionally, Cyxtera is utilized as a co-location data center provider in Santa Clara, California and Vancouver, Canada.
AWS and DD are responsible for operating, managing, and controlling various components of the virtualization layer and storage as well as the physical security and environmental controls of the Public Cloud environments. Cyxtera is responsible for operating physical security and environmental controls of the co-location data center environments. Controls operated by AWS, Dimension Data, and Cyxtera are not included in the scope of this report.

The affected control objective/criteria are included below along with the expected minimum controls in place at AWS, Dimension Data, and Cyxtera.

<table>
<thead>
<tr>
<th>Criteria</th>
<th>Controls expected to be in place</th>
</tr>
</thead>
</table>
| 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 to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality. | AWS, DD, and Cyxtera:  
IT access above least privileged, including administrator access, is approved by appropriate personnel prior to access provisioning.  
Access privileges are reviewed on a quarterly basis by appropriate personnel.  
User additions are authorized by management.  
User access is revoked timely upon termination.  
Users are authenticated via a user account and password before being granted access to the network domain. |
<p>| 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. | |
| 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, and confidentiality. | |</p>
<table>
<thead>
<tr>
<th>Criteria</th>
<th>Controls expected to be in place</th>
</tr>
</thead>
<tbody>
<tr>
<td>CC5.5: Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity’s commitments and system requirements as they relate to security, availability, and confidentiality.</td>
<td></td>
</tr>
<tr>
<td>CC7.4: Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity’s security, availability, and confidentiality commitments and system requirements.</td>
<td>AWS and DD: Changes to system components are authorized, logged, tested, approved and documented before the deployment process.</td>
</tr>
<tr>
<td>A1.1: Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet availability commitments and requirements.</td>
<td>AWS and DD: Backups of system and date are taken periodically Restore tests are performed periodically to ensure data is recoverable in the event of system failure. Monitoring applications are configured to monitor capacity levels and alert appropriate personnel when predefined thresholds are met.</td>
</tr>
<tr>
<td>A1.2: Environmental protections, software, data backup processes, and recovery infrastructure are designed, developed, implemented, operated, maintained, and monitored to meet availability commitments and requirements.</td>
<td>AWS, DD, and Cyxtera: Fire detection and suppression equipment are in place and fire extinguishers have been installed. Data Centers are air conditioned to maintain appropriate atmospheric conditions. Air temperature and humidity are monitored to the appropriate levels. Backup power generators are in place in case of power failure.</td>
</tr>
</tbody>
</table>

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

¹This 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.

**PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS**

Adaptive Insights designs its processes and procedures to meet its objectives for Adaptive Insight’s Business Planning Cloud. Those objectives are based on the service commitments that Workday makes to user entities, the laws and regulations that govern the provision of Adaptive Insight’s Business Planning Cloud Products, and the financial, system, operational and compliance requirements that Adaptive has established for the services.
Workday makes certain Availability, Confidentiality, Privacy, Processing Integrity, and Security representations to its customers as detailed in its Master Subscription Agreement, Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online and within this report. Availability, Confidentiality, Processing Integrity, and Security commitments include, but are not limited to, the following:

- Security and privacy principles within Adaptive Insight’s Business Planning Cloud that are designed for configurable security and compliance with regulations.
- Policies and mechanisms put in place to appropriately secure and segregate Customer Data.
- Regular security monitoring and audits of the environment.
- Use of formal HR business processes such as background checks and Security and Privacy training.
- Monitoring and resolution of system incidents.
- Documentation, testing, authorization, and approval of Software and Operational Changes.
- Maintenance and monitoring of backups to ensure successful replication to meet the service commitments.
- Data integrity and availability monitoring for Production tenants and Production level platform environments.

Adaptive Insights establishes operational requirements that support the achievement of Availability, Confidentiality, Privacy, Processing Integrity, and Security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in 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 Adaptive Insight’s Business Planning Cloud Products.

**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**

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. Workday defines key security and operational roles and responsibilities as follows:

- **Chief Information Officer (CIO)** – Oversees the company’s global information technology (IT) organization, with responsibility for the internal deployment of business technologies and programs that create a competitive advantage for the company and serve as best practices to IT organizations globally.

- **Chief Security Officer (CSO)** – Oversees the information security program and overall security maturity of the business. This includes the identification, evaluation, and prioritization of security related risks and vulnerabilities within the Company’s product, technology and operations. The CSO 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 the Company adhere to applicable global data protection laws, regulations, contractual commitments and privacy compliance requirements.

- **Development (including Product Management) and Quality Assurance** – Responsible for the consistent promotion and development of new products and features, including security features, within the Adaptive Insights applications, as well as manual and automated testing to ensure the quality of software.

- **Products & Technology Release** – The Company’s Product & Technology Release team 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** – The Company 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.
• **Adaptive Insights Hosting Operations** – Responsible for the administration and monitoring of user access to Adaptive Insights’ specific internal systems, administration and management of application, persistent data stores, databases, and operating system (where applicable) availability.

• **Adaptive Insights Support** – Adaptive Insights’ Support team is responsible for responding to and collaborating with Customers when they believe the Adaptive Services is not operating as designed.

• **Internal Audit** – Provides an independent and objective assessment of the Company’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 ISO27001 Information Security Management System (ISMS) requirements. The risk assessment is performed by using the Workday ISO27001 risk assessment as a basis for risk identification, with additional risks that threaten the achievement of the control objectives added as appropriate. As part of this process, threats to security, confidentiality, availability, and integrity of Customer 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, Ethics and Compliance team monitors the effectiveness of the associated programs, including the Privacy program.

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 Security Officer. Issues noted are assessed for criticality and severity, and assigned to the appropriate resources for remediation.

In addition, Workday maintains cyber risk insurance to offset the impact of loss events that would otherwise impair the ability of the entity to meet its objectives.

**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 business strategies and goals with operating performance for its Customers, the Company’s Products & 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 the Adaptive Insights Knowledge Portal. The website contains information which assists Customers with Adaptive Insights Business Planning Cloud. The content is searchable, and the Adaptive Insights Knowledge Portal site includes some of the following:

- Current company and application news and events
- Relevant information to help users understand, navigate, and use the Adaptive Insights system
- Link to login to the support site where Customers are able to ask questions and report problems
- System upgrades and maintenance window status

**Monitoring**

The Hosting Operations team is 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 Workday personnel using a web-based issue tracking tool.

The Company has formally adopted and communicated an Incident Response Plan to identify, document, and remediate incidents which could impact the availability, confidentiality, security or privacy of the environment. Any issues are communicated to the appropriate Company personnel and tracked in an internal web-based issue tracking tool.

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.

An internal issue remediation and improvement opportunity procedure exists to track areas of remediation and/or improvement identified from external compliance assessments. Within this process, Workday performs root cause analysis, assigns follow-up action items and owners to track remediation where appropriate.

The Company also uses automated tools and systems to monitor the security and availability of the Business Planning Cloud, 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.