SOC 3

WorkSpan

System and Organization Controls (SOC) 3

Report of Controls Relevant to
Security, Availability, and Confidentiality
Trust Services Principles

As of March 31, 2019

armanino

Prepared by
ArmaninoLLP's
Risk Assurance & Advisory Practice Group

MANAGEMENT'S ASSERTION REGARDING THE DESIGN AND IMPLEMENTATION OF ITS CONTROLS OVER WORKSPAN'S IT SYSTEM BASED ON THE TRUST SERVICES PRINCIPLES AND CRITERIA FOR SECURITY, AVAILABILITY AND CONFIDENTIALITY.

We, as management of WorkSpan ("WorkSpan" or "the Company") are responsible for designing and implementing effective controls within WorkSpan IT System (system) as of March 31, 2019, to provide reasonable assurance that WorkSpan's service commitments and system requirements relevant to security, availability, confidentiality, and privacy were achieved.

WorkSpan uses service organizations (subservice organizations), Google Cloud Platform("GCP") for hosting and data center services.

WorkSpan designed and implemented effective controls over the security of its IT system to provide reasonable assurance that as of March 31, 2019:

- WorkSpan's IT system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements,
- WorkSpan's IT system was available for operation and use to achieve WorkSpan's commitments and system requirements,
- WorkSpan's IT system information is collected, used, disclosed, and retained to achieve WorkSpan's commitments and system requirements, and

based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy, if the aforementioned subservice organizations maintained effective controls and if user entities applied complementary user entity controls as of March 31, 2019.

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 the system of internal 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

The included Management's Description of Controls (system description) of WorkSpan's IT system identifies the aspects of the System covered by our assertion. The description does not extend to the subservice organizations: Google Cloud Platform. ("GCP") for hosting and data center services.

Joshi M

Milind Joshi

Chief Technology Officer

WorkSpan, Inc.

June 5, 2019

INDEPENDENT SERVICE AUDITOR'S REPORT

To:

The Management of WorkSpan, Inc

Foster City, CA.

We have examined management's assertion that WorkSpan, Inc. (referred to hereafter as "WorkSpan") as of March 31, 2019 designed and implemented effective controls to provide reasonable assurance that:

- WorkSpan's IT system was protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements,
- WorkSpan's IT system was available for operation and use to achieve WorkSpan's commitments and system requirements,
- WorkSpan's IT system information is collected, used, disclosed, and retained to achieve WorkSpan's commitments and system requirements

based on the trust services criteria relevant to security, availability and confidentiality (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria, for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

Service Organization's Responsibilities

WorkSpan is responsible for its service commitments and system requirements and for designing and implementing effective controls within the system to provide reasonable assurance that WorkSpan's service commitments and system requirements were achieved. WorkSpan has also provided the accompanying assertion about the design and implementation of controls within the system. When preparing its assertion, Workspan is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the design and implementation of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were designed and implemented to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. 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. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

Obtaining an understanding of the system and the service organization’s service commitments and system requirements

Assessing the risks that controls were not effective to achieve WorkSpan’s service commitments and system requirements based on the applicable trust services criteria

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Inherent Limitations

There are inherent limitations in the design and implementation of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always be designed and implemented to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the design and implementation of controls is 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, management’s assertion that the controls within WorkSpan’s IT system were designed and implemented as of March 31, 2019, to provide reasonable assurance that WorkSpan’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Armanino LLP

ArmaninoLLP

MANAGEMENT'S DESCRIPTION OF CONTROLS

Company Overview

WorkSpan is a cloud-based software-as-a-service company headquartered in Foster City, CA. We provide an Ecosystem Cloud to our customers to manage their ecosystem relationships. Our customers run their partner programs on WorkSpan to drive revenue growth via build-with, market-with and sell-with initiatives.

WorkSpan was founded in 2014 by Mayank Bawa, Amit Sinha and Milind Joshi. We are funded by Mayfield, Microsoft Ventures, Redline Capital, Knollwood Investment Advisory and Nautilus Ventures. Our customers include SAP, Lenovo, Google, Microsoft and Accenture.

Product Overview

WorkSpan provides an Ecosystem Cloud to our customers to manage their ecosystem relationships. The Ecosystem Cloud consists of the following applications that are used by Alliance and Ecosystem leaders:

- Partner Programs App -- used to manage partner programs, set goals and objectives, track metrics, share files, and collaborate via tasks and messages.
- Sales Plans and Opportunities Apps -- used to manage pre-pipeline and sales pipeline between partners, track contributions, record revenue splits, and calculate incentives.
- Marketing Plans and Activities Apps - used to manage joint marketing calendar, track marketing performance, record budget & expenses, and share marketing materials.
- Solutions Apps - used to manage joint solution readiness process, track solution performance, and share solution materials.
- Assessments Apps - used to assess partnering initiatives and relationships.
- Funds Apps - used to manage proposals, approvals and claims for market development funds between partner companies.

Infrastructure

WorkSpan's Production Application is hosted in the Google Cloud Platform project that is located in the US-Central Region of the Google Cloud Platform.

WorkSpan's information systems have been engineered on the principles of high availability, security and confidentiality. To assist in achieving the desired level of consistency of these principles, WorkSpan has located its production environment within the US-central Region of the Google Cloud Platform - App Engine. Customer facing applications run on servers which participate in an active Disaster Recovery Protocol. These systems are physically and logically secured from other components of the WorkSpan corporate infrastructure.

In case of man-made or natural disaster affecting a Google Cloud data center, data is available in surviving regions, thus mitigating risk of destruction of Google Cloud Data Center in a region. WorkSpan compute resources (Google App Engine) are stateless resources. They are configured to run in a single region, by co-locating with various services. However, in case of disaster, Google

App Engine compute resources can be brought up in any region thus mitigating risk of destruction of Google Cloud Data Center in a region.

GCP also provides data center hosting services. The servers hosted in GCP consist of virtual servers. GCP also provides managed DNS services for internal systems, and short term and long-term data storage for managing the content. Data center facilities are ISO 27001:2013 certified and undergo periodic SOC 1 and SOC 2 Type 2 report audits. Certification status and the results of audits are reviewed periodically as part of WorkSpan’s monitoring controls and the vendor management process.

Software

WorkSpan assembles its SaaS solution from a combination of platform software and custom developed software which are developed by third party companies. Through an iterative process referred to as the Systems Development Life Cycle (SDLC), WorkSpan product team and IT teams works very closely with software development teams to ensure timely and accurate application updates. The WorkSpan Production Application is designed with fault tolerance protection for all layers of the platform and infrastructure, including network traffic and firewalls, as well as the web and application services and backend database connections. The WorkSpan infrastructure is designed to scale substantially to accommodate foreseeable growth in the number of end-users and transaction volume for their products and services.

Data

WorkSpan data is stored in Cloud Data Store and Google Cloud storage (GCS). These are managed multi-region resources. WorkSpan’s data is replicated in real-time and transactionally consistent manner by above services. In case of man-made or natural disaster affecting a Google Cloud data center, data is available in surviving regions, thus mitigating risk of destruction of Google Cloud Data Center in a region.

All sensitive data transmitted and processed within the WorkSpan network is encrypted to protect sensitive data against third-party disclosure in transit. Servers and network components are secured with access control mechanisms and protected by hardened industry standard firewalls and intrusion detection systems. All security services are monitored and updated in a timely manner to address emerging vulnerabilities. WorkSpan application runs on Google App Engine standard environment. Google Cloud platform, uses a variety of isolation and sandboxing techniques for protecting a service from other services running on the same machine.

Application data is stored in Cloud Datastore (https://cloud.google.com/datastore/), and Google Cloud Storage (GCS) in Google Cloud Platform. Cloud Data store is a fully managed, database. Google Cloud Platform automatically handles sharing and replication in order to provide highly available and consistent database. GCS Cloud Storage stores data redundantly, with automatic checksums to ensure data integrity. With Multi-Regional Storage, data is maintained in geographically distinct locations. To minimize service interruption due to hardware failures, natural disasters or other incidents, Google has built a highly redundant infrastructure of data centers.

The automated full data backups are on every day. Backups are stored on an independent GCS bucket, which stores data redundantly.