SYSTEM AND ORGANIZATION CONTROLS 3 REPORT

Apptio Technology Business Management Suite

Description Relevant to Security For The Period
September 1, 2018 To August 31, 2019

Table of Contents

RubinBrown LLP
Certified Public Accountants & Business Consultants

One North Brentwood
Saint Louis, MO 63105

T 314.290.3300
F 314.290.3400

W rubinbrown.com
E info@rubinbrown.com

Section 1. Independent Service Auditor's Report

Independent Service Auditor's Report

Management
Apptio, Inc.
Bellevue, Washington

Scope

We have examined Apptio, Inc.'s (Apptio) accompanying assertion titled "Apptio, Inc.'s Assertion for the Technology Business Management Suite" (assertion) that the controls within the Technology Business Management Suite (TBM Suite or System) were effective throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Apptio's principal service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Apptio uses the following subservice organizations: INAP Corporation (INAP), Equinix, Inc. (Equinix), CenturyLink Communications, LLC (CenturyLink), Westin Building Exchange, Microsoft Corporation – Azure (Azure) and Amazon Web Services (AWS) (collectively, the Subservice Organizations). INAP and Equinix are used for hosting the application and customer data. CenturyLink and Westin Building Exchange are used for hosting corporate services. Azure is used to provide authorization services. AWS is used to provide hosting and authorization services from which Apptio runs the TBM Suite. The description of the boundaries of the System (description) indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Apptio, to achieve Apptio's principal service commitments and system requirements based on the applicable trust services criteria. The description presents the boundaries of Apptio's system. The description does not include any of the controls expected to be implemented at the Subservice Organizations. Our examination did not extend to controls of the Subservice Organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Apptio, to achieve Apptio's principal service commitments and system requirements based on the applicable trust services criteria. Our examination did not extend to such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

Apptio is responsible for its principal service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Apptio's principal service commitments and system requirements were achieved. Apptio has also provided the accompanying assertion about the effectiveness of controls within the System. When preparing its assertion, Apptio 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 effectiveness 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 effective throughout the period to provide reasonable assurance that the service organization's principal 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 principal service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Apptio's principal service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the System were effective to achieve Apptio's principal 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.

Our examination was not conducted for the purpose of evaluating Apptio's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cyber security 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 their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's principal 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 effectiveness 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 Apptio's TBM Suite were effective throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Apptio's principal service commitments and system requirements were achieved based on the applicable trust services criteria, and if the Subservice Organizations and user entities applied the complementary controls assumed in the design of Apptio's controls throughout the period, is fairly stated, in all material respects.

RubinBrown LLP

January 23, 2020

11100 NE 8th St., Suite 600
Bellevue, WA 98004

O +1.425.453.5861
F +1.425.453.1403
www.apptio.com

Section 2. Apptio, Inc.'s Assertion For The Technology Business Management Suite

We, as management of Apptio, Inc. (Apptio), are responsible for designing, implementing, operating, and maintaining effective controls within Apptio's Technology Business Management Suite (TBM Suite or System) throughout the period September 1, 2018 to August 31, 2019 to provide reasonable assurance that Apptio's principal service commitments and system requirements relevant to security for the TBM Suite were achieved.

We are responsible for:

- Identifying the System and describing the boundaries of the System (description), which are presented in Attachment A.
- Identifying our principal service commitments and system requirements, which are presented in Attachment B.
- Identifying the risks that would threaten the achievement of its principal service commitments and service requirements that are the objectives of our System.
- Selecting the trust services categories, presented in Attachment C, that are the basis of our assertion.

Our description of the boundaries of the System is presented in Attachment A and identifies the aspects of the System covered by our assertion.

Apptio uses the following subservice organizations: INAP Corporation (INAP), Equinix, Inc. (Equinix), CenturyLink Communications, LLC (CenturyLink), Westin Building Exchange, Microsoft Corporation – Azure (Azure) and Amazon Web Services (AWS) (collectively, the Subservice Organizations). INAP and Equinix are used for hosting the application and customer data. CenturyLink and Westin Building Exchange are used for hosting corporate services. Azure is used to provide authorization services. AWS is used to provide hosting and authorization services from which Apptio runs the TBM Suite. The description of the boundaries of the System indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Apptio, to achieve Apptio's principal service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the System does not extend to controls of the Subservice Organizations.

The description of the boundaries of the System indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with related controls at Apptio, to achieve Apptio's principal service commitments and system requirements

based on the applicable trust services criteria. The description of the boundaries of the System does not extend to controls of the user entities.

We have performed an evaluation of the effectiveness of the controls within the System throughout the period September 1, 2018 to August 31, 2019, to provide reasonable assurance that Apptio's principal service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*) and included as Attachment C.

Apptio's objectives for the System in applying the applicable trust services criteria are embodied in its principal service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Attachment B.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its principal service commitments and system requirements are achieved.

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 assert that the controls within the System were effective throughout the period September 1, 2018 to August 31, 2019 to provide reasonable assurance that Apptio's principle service commitments and system requirements were achieved based on the applicable trust services criteria.

John Morrow, Chief Administrative Officer and General Counsel

Alain Comeau, Director, Information Security

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Attachment A: Apptio, Inc.'s Description Of Its Technology Business Management Suite

For the period September 1, 2018 to August 31, 2019

Overview

Apptio, Inc. (Apptio or the Company), a wholly owned subsidiary of Vista Equity Partners based in Bellevue, WA, began operations in 2007. The Company develops and sells Technology Business Management (TBM) Suite. The Company's cloud-based platform and applications enable IT leaders to analyze, optimize and plan technology investments.

Types of Service Provided, Types of Data and Applicable Trust Services Criteria

The Security Trust Services Criteria per the TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*AICPA, Trust Services Criteria*) is defined as the applicable trust services criteria for this report. Apptio develops Software-as-a-Service (SaaS) solutions that enable businesses to assess and communicate the cost of Information Technology (IT) services for planning, budgeting and forecasting. The Company's cloud-based applications allow IT leaders to manage, plan and optimize technology investments across on-premises and cloud.

Apptio is focused on helping clients enhance their IT organization and processes through the use of the on-demand TBM Suite product offerings to help IT leaders run IT like a business. The Apptio TBM Suite includes the following products:

- Bill of IT
- Cost Transparency
- IT Benchmarking
- Vendor Insights
- Business Insights
- DataLink
- Interactive Benchmarking
- IT Planning
- FrontDoor
- Cloud Business Management (beginning December 2018)

Apptio provides the TBM Suite SaaS as a Subscription Service that enables IT, Finance and Operations executives to gain visibility into budgets and service costs, make more informed return on investment-based decisions, improve IT operational performance and better communicate the value of IT to the business.

Data

Principle data components are IT cost transactions and reporting. See also the Complementary User Entity Controls for further discussion related to the User Entity responsibilities for cost data transactions and reporting. See also references to Apptio data classification policies and controls in this description.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Apptio is an independent provider of on-demand TBM solutions for managing the business of IT. Apptio enables IT leaders to manage the cost, quality and value of IT services by providing visibility into the total cost of IT services, communicating the value of IT to the business through an interactive Bill of IT and strategically aligning the planning, budgeting and forecasting processes. Apptio's TBM Suite solutions play a role in helping companies understand and drive chargeback, virtualization, cloud and other key technology initiatives.

Infrastructure

Apptio has outsourced data center hosting to INAP Corporation, Equinix, Inc. and Amazon Web Services. Apptio also uses CenturyLink Communications, LLC and Westin Building Exchange facilities for hosting corporate services. Microsoft Corporation - Azure is used to provide authentication services.

Monitoring of Subservice Organizations

The Information Security Team reviews the SOC reports from the Subservice Organizations to evaluate the effectiveness of their controls over physical security and environmental controls.

Control Environment

Apptio's control environment reflects the philosophy of senior management concerning the importance of security of client data and information. Apptio's Security Council oversees the security activities of Apptio. The Council members are from each of the business lines. The Council is charged with establishing overall security policies and procedures for Apptio. The importance of security is emphasized within Apptio through the establishment and communication of policies and procedures and is supported by investment in resources and people to carry out the policies. In designing its controls, Apptio has taken into consideration the relevance of controls to meet the applicable trust services criteria.

Internal control activities help ensure management's directives are carried out. Preventative and detective controls are in place and documented for information processing and IT. Management has placed in operation a Data Classification and Handling Policy to direct employees on the manner in which company and client data is managed.

Governance and People

Apptio is dedicated to conducting business in an ethical manner and fosters a culture dedicated to strong values and high standards.

Apptio's Board of Directors provides oversight to Apptio and is comprised of seven members, some of whom are independent of Apptio. Board membership is composed of individuals with significant experience in IT and business.

Apptio is comprised of business units focused on providing clients the information they need to make informed decisions around their respective IT environments. These business units work together to deliver results which allow clients to have transparency into their IT environment, perform appropriate IT planning and budget spend analysis and maximize their return on investment in IT.

Information Security Function

Security awareness is an important part of Apptio's overall security posture. Apptio has a dedicated Information Security Team within the organization. The Information Security team's main responsibilities are risk governance, audit and compliance, access control, company security awareness and to protect the integrity and availability of confidential information, including customer data.

Apptio has based its security framework on ISO 27001 standards, which is an international practice standard for Information Security Management.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Procedures

Management has developed, and communicated to employees and contractors, procedures to ensure the security over the services. Changes to these procedures are only done after authorization by management. These procedures cover the following key security lifecycle areas:

- Data classification and life cycle (data at rest, in motion)
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary back-ups
- Incident response
- Maintenance of restricted access to system configurations, superuser functionality, master passwords, powerful utilities and security devices (for example, firewalls)

Risk Management Process

Apptio has established an enterprise-wide process to mitigate risk. Management reviews risk-related reporting for internal operations and for Subservice Organizations and takes corrective action where needed. Apptio uses a qualitative/quantitative hybrid method to determine areas of risk, likelihood and business impact.

Information and Communication Systems

Client Communications

Apptio and clients execute a contract prior to on-boarding new clients. Apptio posts the system description to internal and external websites. Commitments to, and obligations of, customer users are communicated, published and available to customers and internal users.

Internal Communication

Apptio management supports effective communication with personnel to help ensure employees understand their individual roles and responsibilities. Organizational values and behavioral standards are communicated to employees and are captured in Apptio's *Employee Handbook*. Policies and procedures are available in the operations areas to guide employees in the performance of their duties.

Apptio has a set of information security policies to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the communication of time-sensitive information and processes for security and system availability purposes that notify key personnel in the event of problems.

Security Management

Apptio understands that one of its key responsibilities is around the protection of customer data. Customer data is classified for appropriate data handling. Apptio's customer data is handled with the utmost of care and it is classified within the highest tier of Apptio's data classification policy.

User entities manage notification and consent requirements and maintain accuracy of the data. Apptio processes user entity data only in accordance with contractual agreements.

Apptio has a dedicated Information Security Team responsible for management of information security throughout the organization.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

The Information Security Team maintains security, monitors for known incidents and patches, as well as results from recent vulnerability assessments, and addresses necessary changes to the policies and procedures. Such changes can include a reclassification of data, a reassessment of risk, changes in incident response plans and a verification of responsibilities for authorizing and monitoring accesses.

Complementary Subservice Organization Controls

Apptio utilizes various subservice organizations to provide co-location space and Platform-as-a-Service. Apptio's controls related to the TBM Suite cover only a portion of overall internal control for each client of Apptio. It is not feasible for the controls to be achieved solely by Apptio. It is expected that the Subservice Organizations have implemented the controls to support achievement of the principal service commitments and system requirements based on the applicable trust services criteria, which are the Common Criteria (CC), as described below.

The following is a table associated with the controls at the Subservice Organizations that provide co-location space:

	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
1.	Subservice organizations are responsible for maintaining proper oversight over the respective subservice employees and activities.	CC1.3
2.	Subservice organizations are responsible for ensuring physical access to computer resources is restricted appropriately.	CC6.4
3.	Subservice organizations are responsible for ensuring that system availability (including data center environmental controls) is monitored and issues are identified and resolved.	CC7.2

The following is a table associated with the controls at the Subservice Organization that provides Platform-as-a-Service:

	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
1.	Subservice organization is responsible for maintaining proper oversight over the respective subservice employees and activities.	CC1.3
2.	Subservice organization is responsible for ensuring that activities are properly logged, monitored and available for management review.	CC6.1
3.	Subservice organization is responsible for ensuring that logical access to underlying infrastructure is restricted appropriately and that a logical separation exists between Apptio data and access by subservice organization personnel.	CC6.1 CC6.2 CC6.3
4.	Subservice organization is responsible for ensuring physical access to computer resources is restricted appropriately.	CC6.4

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
5.	Subservice organization is responsible for ensuring that system availability (including cloud infrastructure) is monitored and issues are identified and resolved.	CC7.2
6.	Subservice organization is responsible for ensuring that system availability (including data center environmental controls) is monitored and issues are identified and resolved.	CC7.2
7.	Subservice organization is responsible for ensuring that changes to software and hardware used to provide the cloud infrastructure is authorized, tested and approved prior to being placed in operation.	CC8.1

Complementary User Entity Controls

Apptio's services were designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Apptio's controls. The user entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user entities.

User entities of Apptio's system should maintain controls to provide reasonable assurance that the following requirements are met for the specified CC:

1. Clients are responsible for ensuring that the reports generated out of the TBM Suite accurately reflect the data the clients upload into the service. (CC2.1)
2. Clients are responsible for reporting identified or suspected security incidents to Apptio on a timely basis. (CC2.2)
3. Clients are responsible for assigning an Administrator to be responsible for coordinating, communicating, and monitoring any changes made which may affect the input, output and security of client's transformed data. (CC6.1, CC6.2, CC6.3, CC8.1)
4. Clients are responsible for assigning an Administrator who is responsible for monitoring and maintaining their security assignments within their instance. (CC6.1)
5. Clients are responsible for assigning to each on-line account, a unique account identification to positively identify the user, a password following industry standard password complexity rules and a role to facilitate segregating assigned duties. (CC6.1)
6. Clients are responsible for periodically changing passwords to maintain the secrecy of each account password. (CC6.1)
7. Clients are responsible for periodically certifying user access to verify that security levels are appropriate for each account and to identify any potential segregation of duties conflicts. (CC6.1, CC6.2, CC6.3)
8. Clients are responsible for reviewing reports requested from Apptio to evaluate user/operator errors and attempts to access unauthorized functions. (CC6.1)

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

9. Clients are responsible for ensuring appropriate account management and accuracy. This includes ensuring all client accounts are appropriately approved, terminations of client accounts are accurate and timely, and changes in access levels are all handled according to the client's access management policies and procedures. (CC6.1, CC6.2, CC6.3)

10. Clients are responsible for providing security protections and updated software to each user's operating systems and web browsers used to access the Apptio platform. (CC6.1, CC6.8, CC7.2)

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Attachment B: Principal Service Commitments And System Requirements

Security commitments to user entities are documented and communicated in Customer Agreements, as well as in the description of the service offering provided online.

Only the principle service commitments and system requirements relevant to the applicable trust services criteria are within the boundaries of the system.

Apptio will comply with its current Security Framework over safeguards for the TBM Suite designed to protect against accidental or unauthorized access of data properly loaded to the Subscription Service. Such efforts will be Apptio's sole obligation with respect to security and protection of User Entity data as it is processed or stored on a computer and/or computer network owned or controlled by Apptio in connection the Subscription Service.

The Security Framework covers the following areas for a broad set of user entities: Network Security, Physical Security, Application Security, Security Notifications and Evaluation. Please also see the Complementary Subservice Organization Controls Section listed within Attachment A, which further discuss the dependences on these Subservice Organizations to allow Apptio to meet its principle system requirements and service commitments.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Attachment C: AICPA Trust Services Criteria

This attachment includes the AICPA trust services criteria, included in the scope of the engagement, relevant to security set forth in *TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Trust Services Criteria	Criteria Description
CC1.0 Control Environment	
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.
CC2.0 Communication and Information	
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.
CC3.0 Risk Assessment	
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Trust Services Criteria	Criteria Description
CC4.0 Monitoring Activities	
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.
CC5.0 Control Activities	
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.
CC6.0 Logical and Physical Access Controls	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403

Trust Services Criteria	Criteria Description
CC7.0 System Operations	
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.
CC8.0 Change Management	
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.
CC9.0 Risk Management	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.

11100 NE 8th St., Suite 600 · Bellevue, WA 98004 · Office 425.453.5861 · Fax 425.453.1403