SYSTEM AND ORGANIZATION CONTROLS 3 REPORT
Apptio Technology Business Management Suite

Description Relevant to Security For The Period
September 1, 2017 To August 31, 2018

TABLE OF CONTENTS

ASSERTION OF MANAGEMENT

APPTIO®

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

O +1.425.453.5861
F +1.425.453.1403
www.apptio.com

Assertion By the Management of Apptio, Inc. for Apptio's Technology Business Management Suite

We, as management of Apptio Inc. (Apptio), are responsible for designing, implementing, operating and maintaining effective controls within the Apptio Technology Business Management Suite (TBM or System) throughout the period September 1, 2017 to August 31, 2018 to provide reasonable assurance that Apptio's service commitments and system requirements relevant to security for the TBM Suite were achieved.

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, CenturyLink Communications, LLC (CenturyLink), Westin Building Exchange 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. AWS is used to provide cloud hosting and authorization services from which Apptio runs the TBM Suite. The description of the boundaries of the System excludes the applicable trust services criteria and related controls of the Subservice Organizations. The description of the boundaries of the System also indicates that certain applicable trust services criteria specified in the description of the boundaries of the System can be met only if complementary subservice organization controls assumed in the design of Apptio's controls are suitably designed and operating effectively, along with the related controls at Apptio. 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 applicable trust services criteria specified in the description of the boundaries of the System can be met only if complementary user entity controls assumed in the design of Apptio's controls are suitably designed and operating effectively, along with related controls at the service organization and the Subservice Organizations. 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, 2017 to August 31, 2018, to provide reasonable assurance that Apptio's 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 100A, *2016 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Apptio's objectives for the System in applying the applicable trust services criteria are embodied in its 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 in security controls, a service organization may achieve reasonable, but not absolute, assurance that its 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, 2017 to August 31, 2018 to provide reasonable assurance that Apptio’s service commitments and system requirements were achieved based on the applicable trust services criteria.

Alain Comeau

Kurt Shintaffer, Chief Financial Officer

Alain Comeau, Director, Information Security

ATTACHMENT A

APPTIO INC.’S DESCRIPTION OF THE BOUNDARIES OF ITS TECHNOLOGY BUSINESS MANAGEMENT SUITE (SYSTEM)

APPTIO INC.'S DESCRIPTION OF THE BOUNDARIES OF ITS TECHNOLOGY BUSINESS MANAGEMENT SUITE

For the period September 1, 2017 to August 31, 2018

Overview

Apptio, Inc. (Apptio), a global enterprise based in Bellevue, WA, began operations in 2007 and entered the public markets in an initial public offering in September 2016. Apptio has demonstrated momentum across its business. The company's revenues have grown significantly with customers across all industries.

Apptio is focused on helping clients enhance their Information Technology (IT) organization and processes through the use of the on-demand suite of Technology Business Management (TBM) 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 and IT Planning. Apptio provides the TBM Suite as a Software-as-a-Service (SaaS) that enable 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.

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.

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 committee members are from each of the business lines. The committee 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 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, three 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. These business units include Sales (Revenue), People and Culture, Marketing, Customer Operations / Success, Corporate Development, Finance, and Products and Engineering.

Information Security Function

Security awareness is an important part of Apptio's overall security posture. Apptio has a dedicated Information Security function within the organization. This function's main responsibilities are risk governance, audit and compliance, access control, company security awareness, and to protect the confidentiality, integrity and availability of confidential information, including Customer Data which is classified within the highest tier within the Data Classification policy.

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

Procedures

Management has developed, and communicated to employees, 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

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.

Subservice Organizations

Apptio has outsourced data center hosting to co-location providers, and is using Amazon Web Services (AWS) as a Platform-as-a-Service. These together create a hybrid cloud environment that maximizes the benefits of both, with information security as a primary consideration in the overall architecture and design. Within the co-location datacenter, each customer has their own unique virtual instances supporting web applications and customer databases. At AWS, the web and application tiers are multi-tenant and the backend database is unique for each customer. In both cases, the data is encrypted at rest and secured via a defense in depth.

Apptio relies on the hosting facilities to provide physical security, power, space and other environmental protections. These facilities have their own formal policies and procedures in place for providing physical security.

Infrastructure support access is achieved via a secured VPN connection using two-factor authentication and also requires an SSH encrypted session.

To access any of the services provided, clients must purchase a subscription (contract) and the client's access must be pre-provisioned.

Security Management

Data Security

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.

Logical Security

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

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. It is expected that the subservice organizations have implemented the controls to support achievement of the 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.	CC1.1
2.	Subservice organizations are responsible for ensuring physical access to computer resources is restricted appropriately.	CC5.5
3.	Subservice organizations are responsible for ensuring that system availability (including data center environmental controls) is monitored and issues are identified and resolved.	CC6.1

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.	CC1.1
2.	Subservice organization is responsible for ensuring that activities are properly logged, monitored and available for management review.	CC5.1
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.	CC5.1 CC5.2 CC5.4
4.	Subservice organization is responsible for ensuring physical access to computer resources is restricted appropriately.	CC5.5
5.	Subservice organization is responsible for ensuring that system availability (including cloud infrastructure) is monitored and issues are identified and resolved.	CC6.1
6.	Subservice organization is responsible for ensuring that system availability (including data center environmental controls) is monitored and issues are identified and resolved.	CC6.1
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.	CC7.4

Complementary User Entity Controls

Apptio's services were designed with the assumption that certain controls would be implemented by user entities to achieve the service commitments and system requirements based on the applicable trust services criteria relevant to Security, which are the CC supporting the Apptio TBM Suite. 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 reporting identified or suspected security incidents to Apptio on a timely basis. (CC 2.5)
2. 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. (CC 5.1, 5.2, 5.4, 7.1-7.4)
3. Clients are responsible for assigning an Administrator who is responsible for monitoring and maintaining their security assignments within their instance. (CC 5.1)

4. 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. (CC 5.1)
5. Clients are responsible for periodically changing passwords to maintain the secrecy of each account password. (CC 5.1)
6. 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. (CC 5.1, 5.2, 5.4)
7. Clients are responsible for reviewing reports requested from Apptio to evaluate user/operator errors and attempts to access unauthorized functions. (CC 5.1)
8. 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. (CC 5.1, 5.2, 5.4)
9. 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. (CC 5.1, 5.8, 6.1)

ATTACHMENT B
PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Principal Service Commitments and System Requirements

Apptio designs its processes and procedures related to the System to meet its objectives for its TBM services. Those objectives are based on the service commitments that Apptio makes to user entities and the related 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. Base security commitments include, but are not limited to, the following:

- Security principles within the fundamental designs of the TBM Suite that are designed to permit system users to access the information for their entity while restricting them from accessing information of other entities.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of firewalls and network segmentation restricting traffic flow to appropriate traffic.
- Logical access controls and regular review / monitoring.
- Security monitoring infrastructure including intrusion detection, centralized log management, and alerting.
- Geographically separated data centers with multi-layered physical security.
- Vulnerability Management program designed to identify and correct vulnerabilities within the environment in a timely manner.
- Incident Response program designed to minimize the impact and protect resources.

Apptio establishes operational requirements that support the achievement of security commitments and other system requirements. Such requirements are communicated in Apptio’s 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 the TBM Suite.

REPORT OF INDEPENDENT SERVICE AUDITOR

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

Independent Service Auditor's Report

Management
Apptio
Bellevue, Washington

Scope

We have examined Apptio, Inc.'s (Apptio) accompanying assertion titled "Assertion of the Management of Apptio, Inc. for Apptio's Technology Business Management Suite" (assertion) that the controls within the Technology Business Management Suite (TBM or System) were effective throughout the period September 1, 2017 to August 31, 2018, to provide reasonable assurance that Apptio's 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 100A, *2016 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Trust Services Criteria).

Apptio uses the following subservice organizations: INAP Corporation (INAP), Equinix, CenturyLink Communications, LLC (CenturyLink), Westin Building Exchange 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. AWS is used to provide cloud hosting and authorization services from which Apptio runs the TBM Suite. The description indicates that certain applicable trust services criteria can be met only if complementary subservice organization controls assumed in the design of Apptio's controls are suitably designed and operating effectively, along with the related controls at Subservice Organizations. 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 of the boundaries of the System (description) indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Apptio's controls are suitably designed and operating effectively, along with related controls at the service organization. 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 service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Apptio's 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 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 Apptio’s 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 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 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 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 System were effective throughout the period September 1, 2017 to August 31, 2018, to provide reasonable assurance that Apptio’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

RubinBrown LLP

January 7, 2019