APPTIO®

SYSTEM AND ORGANIZATION CONTROLS 3 REPORT
Apptio Technology Business Management Suite

Description Relevant to Security For The Period
September 1, 2016 To August 31, 2017

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 OF APPTIO MANAGEMENT FOR APPTIO'S BUSINESS TECHNOLOGY MANAGEMENT SUITE

We, as management of 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, 2016 to August 31, 2017 to provide reasonable assurance that Apptio's service commitments and system requirements relevant to security for the TBM Suite were achieved.

The timing and period of coverage for each of Apptio's products included within the TBM Suite can be found in the table below:

Product	Period Covered
Cost Transparency Bill of IT IT Benchmarking Business Insights DataLink Legacy IT Planning Interactive Benchmarking	June 1, 2017 through August 31, 2017
IT Planning FrontDoor	September 1, 2016 through August 31, 2017

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: Internap, Metronode, Equinix, Level 3 Communications, LLC, Westin Building Exchange and Amazon Web Services (AWS) (collectively, the Subservice Organizations). Internap, Metronode and Equinix are used for hosting the application and customer data, which includes physical security. Level 3 Communications, LLC and Westin Building Exchange are used for hosting corporate services, which includes physical security. AWS is used to provide cloud hosting and authorization services from which Apptio runs the TBM Suite, which includes various controls in support of security. The description of the boundaries of the System includes only the applicable trust services criteria and related controls of Apptio and 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 our controls are suitably designed and operating effectively, along with the related controls at the service organization. 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 the 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, 2016 to August 31, 2017, 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, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and System requirements are achieved.

We assert that the controls within the System were effective throughout the period September 1, 2016 to August 31, 2017 to provide reasonable assurance that Apptio's service commitment and System requirements were achieved based on the applicable trust services criteria.

Signature: ____________________
Name: Kurt Shintaffer
Title: Chief Financial Officer

Signature: ____________________
Name: Alain Comeau
Title: Director, Information Security

ATTACHMENT A

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

APPTIO’S DESCRIPTION OF THE BOUNDARIES OF ITS TECHNOLOGY BUSINESS MANAGEMENT SUITE

For the period September 1, 2016 to August 31, 2017

Overview

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, Business Insights, DataLink 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.

Apptio is determined to provide its customers with assurance that the data within the hosting environment is handled appropriately and that the environment itself has mechanisms in place to ensure its safety. The timing and period of coverage for each of Apptio’s products included within the TBM Suite can be found in the table below:

Table 1

Product	Period Covered
Cost Transparency Bill of IT IT Benchmarking Business Insights DataLink Legacy IT Planning Interactive Benchmarking	June 1, 2017 through August 31, 2017
IT Planning FrontDoor	September 1, 2016 through August 31, 2017

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 meets quarterly and reports to the board annually. The committee, under the direction of the Apptio board, 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 relevant trust services criteria.

Internal control activities help ensure management’s directives are carried out. Such activities include top level review of actual performance and management reviews at the function or activity level. Controls are in place and documented for information processing and IT. Apptio has implemented preventive, detective and corrective control activities across the entity and specifically the production environment to protect the receipt, processing and the storage of transformed client data. Management 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.

A Board of Directors provides oversight to Apptio by reviewing financial and operational results. This Board is comprised of seven members, three of whom are independent of Apptio. Board membership is composed of individuals with significant industry and business experience.

Executive leadership regularly discusses the operational and financial performance of the company. Management reviews reports on IT general and physical security controls provided by independent parties. Management has documented a Data Classification and Handling policy, which covers both Apptio and customer data.

Apptio is comprised of business units focused on providing clients the information they need to make informed decisions around their IT environment. These business units work together to deliver results which allow clients with transparency into their IT environment, perform appropriate IT planning and budget spend analysis, and maximize their return on investment in IT. Budgets are analyzed for necessary resources by management annually. These business units include Sales (Revenue), People and Culture, Marketing, Customer Operations / Success, Corporate Development, Finance, and Products and Engineering.

Background Checks

Background checks are performed on new employees, who are also required to review and acknowledge their receipt of relevant security policies. Positions are supported by job descriptions. Employees are subject to Apptio procedures for accessing systems, potential consequences for violating Apptio's information security policy, and related disciplinary action. Employees are instructed to report potential security incidents to the Information Security team. Apptio's customer agreements instruct user entities and clients to notify their respective account representative if they become aware of a possible security breach.

Training

New employees sign employment commitments (Non Disclosure Agreements, Security Policy Acknowledgements, Contracts and/or employee agreements). Policies and procedures providing guidance and direction are communicated to employees.

Security awareness is an important part of Apptio's overall security posture. Personnel, regardless of position, are required to sign off that they have read and agree to adhere to Apptio Security Policies as well as the Code of Conduct upon hire. They also are required to attend an Information Security led discussion around data protection and security practices at Apptio as well as complete online security awareness training. Annually thereafter, personnel are required to review the online security awareness training and resubmit their acknowledgement of awareness and compliance.

Apptio code developers are required to complete additional annual trainings that center on secure coding and development practices, which include subject matter from the Open Web Application Security Project (OWASP) Top Ten and other leading secure coding practice methodologies.

Information Security Function

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.

Security Policies

The Information Security team maintains security certifications and are required to annually sign and acknowledge their review of the information security policies. They are responsible for developing, maintaining, and enforcing Apptio's information security policies. The information security policies are reviewed and approved annually by the Director of Information Security. Apptio policies include probation, suspension and termination as potential sanctions for employee misconduct.

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 providers and takes corrective action where needed. Apptio uses a qualitative/quantitative hybrid method to determine areas of risk, likelihood and business impact. Apptio employs formal and informal risk assessment procedures. Management proactively manages the risks identified through communication meetings with Apptio's Security Council, comprised of executive leaders whose roles and/or job functions provides management direction and a sounding board for Apptio's information security initiatives which directly influences the security posture of the company. Additionally, Apptio regularly works directly with clients to manage industry related risks.

Apptio regularly reviews the risks that may threaten the achievement of the criteria for the security principle set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (2016)* (AICPA, *Trust Services Principles*).

Senior management, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Apptio's security policies.

Regular internal scans and penetration tests are performed and evaluated by the Information Security team. Annual control self-assessments as well as annual third-party audits and penetration testing are performed over the operating environment. (See Monitoring section below). Changes in security threats and risks are reviewed by Apptio and updates to existing control activities and information security policies are performed as necessary. Potential threats identified during the risk assessment are analyzed and a mitigation plan is developed in accordance with policy.

Information and Communication Systems

Client Communication

Users have been provided with information on how to report security failures, incidents, concerns, and other complaints to Apptio. Procedures on how to identify and escalate potential customer data security breaches have also been developed and communicated to all relevant internal parties.

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.

Monitoring

Apptio's infrastructure services are actively monitored on a real-time basis through the implementation of outside-in service probes and inside-out service watchdogs. Logging and monitoring software is used to collect data from system components and used to monitor system performance, potential security threats, vulnerabilities, resource utilization, and to detect unusual system activity. Apptio has deployed automated monitoring tools to monitor and track security events. In addition to the daily oversight, monthly vulnerability assessments, and use of logging and monitoring software, management provides further security monitoring through other periodic and ad-hoc internal audits conducted by the Information Security team. Also, Apptio engages with a third party on an annual basis to conduct penetration tests and application vulnerability scans.

Apptio utilizes service host-level monitoring. Apptio's applications separate system, request and audit logs, which are indexed for reporting. A combination of off-the-shelf tools and custom code are used for outside-in monitoring of all services and more comprehensive inside-out monitoring of all services. Both AWS CloudTrail and AWS CloudWatch are consumed into central monitoring services to ensure Application Program Interface (API) calls and performance information is collected, reviewed and alerted on.

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.

Monitoring of Subservice Organizations

The Information Security team reviews third party audit / SOC reports from contracted co-location facilities and the third party hosting service (AWS) to evaluate the effectiveness of their controls over physical security and environmental controls on an annual basis. Apptio also has processes and controls in place to address the complementary user entity controls identified in each subservice organization's description of its systems.

This description of the boundaries of the System does not include controls of those subservice organizations. Apptio's controls include only the controls of Apptio and exclude the controls of the data center hosting subservice organizations. The description of the boundaries of the System has been prepared by Apptio management to provide relevant information related to the TBM Suite.

Throughout its daily operational activities, Apptio management monitors the services performed by the subservice organizations to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively. Management also holds periodic calls and performs walkthroughs with the subservice organization to monitor compliance with the service level agreement, stay abreast of changes planned at the subservice organization, and relay any issues or concerns to the subservice organizations' management.

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. Internal vulnerability tests are conducted at least quarterly, using commercially available products and external third-party tests are conducted at least annually. Vulnerabilities discovered are remediated in accordance with policy. 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.

Additionally, Information Security is responsible for monitoring third-party controls and for updating the annual IT risk assessment.

Apptio has implemented role-based security to limit and control access within the services. Apptio employees are granted logical access to systems based on approvals by appropriate personnel. The ability to create or modify user access accounts and user access privileges is limited to authorized personnel. User access is reviewed quarterly by the respective product management to verify whether individuals' access is necessary for their job functions and to identify the existence of inappropriate accounts.

The Human Resources (HR) department opens a ticket with IT personnel to notify them of terminations. IT adjusts privileges and ensures access has been appropriately removed or disabled.

Administrative access to production servers and databases is restricted to authorized employees. Remote access to system administrative capabilities requires multi-factor authentication and occurs over an encrypted VPN connection.

Unique user identification numbers, names and passwords are required to authenticate all users to Apptio applications, as well as to the underlying infrastructure services. Password parameters consist of the following:

- Passwords must contain a minimum number of characters
- Passwords must be complex
- Passwords expire after a prescribed number of days
- Reuse of passwords is restricted.

This does not apply to customers who have opted to leverage Single-Sign-On (SSO) and who are leveraging their own password policies. For Apptio personnel access to the application, SSO is established to the application and mapped to an Apptio identity provider service.

A network perimeter security system is in operation. Apptio's production environments utilize a standard 3-tier system. Access to firewalls is limited to authorized network personnel only. Firewalls function on a deny-by-default policy and only have rules to allow authorized traffic through, and are configured using a mostly closed configuration with open ports only where required. Any public packet coming in is forced to utilize HTTPS/TLS with AES-256 bit encryption. Entity policies prohibit the transmission of sensitive information over the Internet or other public communications paths unless it is encrypted. The Apptio TBM Suite allows access to authenticated users only. External connections to the Apptio TBM Suite are encrypted.

Apptio servers and workstations have Anti-Virus / Anti-Malware utilities installed. These systems are centrally managed and checks for new definition updates occur daily.

Apptio also utilizes a Host-based Intrusion Detection System (HIDS) on all hosts. All of the data generated from these services are centrally stored within a centralized logging and notification system.

Apptio uses custom hardening guidelines when implementing new servers and equipment. These rules include items such as removing unneeded packages and services, removing or disabling default accounts, and setting up configurations for real-time, centralized system management. The rules are based on industry standard best practices for hardening systems. Apptio configures the system to provide only essential capabilities in accordance with Apptio infrastructure and software hardening procedures. These hardening guides are reviewed and reapproved on an annual basis.

Physical Security and Environmental Controls

Information at Apptio is considered an asset to be protected. Management has placed controls in operation regarding physical access to their primary Corporate facility and local computing resources. Apptio has an access card security system in operation to restrict physical access to computer resources and to the Corporate (HQ) facility. Requests for access to the Bellevue Corporate facility are made, approved, and communicated through a ticketing system. An annual process to review user access to the HQ facility and HQ server room is in place to help ensure access is appropriate. Management reviews third party reports to determine that physical security safeguards are in place for Apptio's computing resources.

The Human Resources (HR) department opens a ticket with IT personnel to notify them of terminations. IT adjusts privileges and ensures access has been appropriately removed or disabled.

System Operations

Incident Response

The Security Administration team uses a variety of security utilities to identify and detect possible security threats and incidents. These utilities include, but are not limited to, firewall notifications, HIDS alerts, vulnerability assessment reports, and operating system event logs. Logging and monitoring software is used to collect data from system components and used to monitor system performance, potential security threats, vulnerabilities, resource utilization, and to detect unusual system activity.

Security incidents and other IT-related problems are reported to the Information Security team. Issues are tracked using a ticket and monitored until remediated or mitigated.

Internal and external users have been provided with information on how to report security failures, incidents, concerns, and other complaints to Apptio. Security and operations personnel monitor the system for security failures and incidents. Customer Support personnel follow defined protocols when they identify security concerns. Apptio has established documented policies and procedures for incident management, which address both digital and physical security incidents. In the event of an incident, this defined process outlines the various phases in managing the incident, to include notification of the affected parties, proper containment/mitigation and executive level involvement. Internal and external users are informed of security incidents in a timely manner and advised of corrective measure to be taken on their part. For high severity security incidents, a root cause analysis is prepared and reviewed by management. Based on the root cause analysis, change requests are prepared.

In the event Apptio has actual, confirmed knowledge of any unauthorized access to or acquisition of Client Data in a manner that renders misuse of the information reasonably possible, Apptio will, subject to an any applicable laws, (a) promptly notify affected customers as required by applicable law and (b) take commercially reasonable measures to address the incident in a timely manner.

Data Backup and Recovery
Automatic backups are performed on a daily basis. At least quarterly, disaster recovery tests are performed to further help ensure existing backups are usable in accordance with Apptio's procedures. This ensures a smooth transition of service in the event of a possible failure with any datacenter.

Change Management
Apptio has a formalized change management process in place which requires at a minimum that the following occurs:

1. Identification and recording of changes in a centralized tracking system.
2. Assessment of risk and potential effect of such changes.
3. Approval of proposed changes by an appropriate level of management.
4. For software changes:
   a. Code review performed by peers to ensure quality of code and secure coding practices were followed.
   b. Static code analysis to determine whether secure coding practices were followed.
   c. Automated and manual testing of code changes to verify operational functionality pre-release.
5. A formalized release management or deployment process.
6. Roll back plans are established for changes to production.
7. Post implementation verification.

Changes to software are developed and tested in a separate development or test environment before implementation where possible. Additionally, only authorized personnel have the ability to migrate changes into production environments. Changes to the system are communicated internally as well as externally when an end-user's responsibilities are significantly impacted or when the change represents a material change to the functionality or security of the system.

Emergency changes follow a similar change management process, but at an accelerated timeline.

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 associated Trust Services Criteria and related criteria relevant to Security 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

	Complementary Subservice Organization Controls (CSOCs)	Related Trust Services Criteria
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 applicable Trust Services Criteria and related criteria relevant to Security which are the Common Criteria (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:

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, processing, 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.

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.

REPORT OF INDEPENDENT SERVICE AUDITOR

Independent Service Auditor's Report

Management
Apptio
Bellevue, Washington

Scope

We have examined Apptio’s accompanying assertion titled "Assertion of the Management of Apptio 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, 2016 to August 31, 2017, 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). 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.

Apptio uses the following subservice organizations: Internap, Metronode, Equinix, Level 3 Communications, LLC, Westin Building Exchange and Amazon Web Services (AWS) (collectively, the Subservice Organizations). Internap, Metronode and Equinix are used for hosting the application and customer data, which includes physical security. Level 3 Communications, LLC and Westin Building Exchange are used for hosting corporate services, which includes physical security. AWS is used to provide cloud hosting and authorization services from which Apptio runs the TBM Suite, which includes various controls in support of security. 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 Apptio's system; its controls relevant to the applicable trust services criteria; and the types of controls that the service organization expects to be implemented, suitably designed, and operating effectively at the subservice organization to meet certain applicable trust services criteria. The description does not include any of the controls expected to be implemented at the subservice organization. Our examination did not extend to controls of the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization 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, 2016 to August 31, 2017, 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

March 26, 2018