PLANVIEW, INC.

SOC 2 REPORT

FOR

SPIGIT

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON CONTROLS RELEVANT TO SECURITY AND AVAILABILITY

MARCH 16, 2019, TO OCTOBER 31, 2019

Attestation and Compliance Services

This report is intended solely for use by the management of Planview, Inc., user entities of Planview, Inc.'s services, and other parties who have sufficient knowledge and understanding of Planview, Inc.'s services covered by this report (each referred to herein as a "specified user").

If report recipient is not a specified user (herein referred to as a "non-specified user"), use of this report is the non-specified user's sole responsibility and at the non-specified user's sole and exclusive risk. Non-specified users may not rely on this report and do not acquire any rights against Schellman & Company, LLC as a result of such access. Further, Schellman & Company, LLC does not assume any duties or obligations to any non-specified user who obtains this report and/or has access to it.

Table of Contents

SECTION I

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Planview, Inc.:

Scope

We have examined Planview, Inc.'s ("Planview" or the "service organization") accompanying description of its Spigit system, in Section 3, throughout the period March 16, 2019, to October 31, 2019, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 16, 2019, to October 31, 2019, to provide reasonable assurance that Planview's service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Planview uses various subservice organizations for data center hosting, encrypted data backup storage, and embedded business reporting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Planview, to achieve Planview's service commitments and system requirements based on the applicable trust services criteria. The description presents Planview's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Planview's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The information included in Section 5, "Other Information Provided by Planview" is presented by Planview management to provide additional information and is not a part of the description. Information about Planview's management's responses to exceptions noted has not been subjected to the procedures applied in the examination of the description, the suitability of the design of controls, and the operating effectiveness of the controls to achieve Planview's service commitments and system requirements based on the applicable trust services criteria.

Service Organization's Responsibilities

Planview 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 Planview's service commitments and system requirements were achieved. Planview has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Planview is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements;
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively;
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria;
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria;
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria; and
- Evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual users may consider important to meet their informational needs.

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 are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating 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.

Description of Test of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section 4 of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects,

a. the description presents Planview's Spigit system that was designed and implemented throughout the period March 16, 2019, to October 31, 2019, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period March 16, 2019, to October 31, 2019, to provide reasonable assurance that Planview's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations applied the complementary controls assumed in the design of Planview's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period March 16, 2019, to October 31, 2019, to provide reasonable assurance that Planview's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Planview's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section 4, is intended solely for the information and use of Planview; user entities of Planview's Spigit system during some or all of the period March

16, 2019, to October 31, 2019, business partners of Planview subject to risks arising from interactions with the Spigit system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization;
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties;
- Internal control and its limitations;
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements;
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services;
- The applicable trust services criteria; and
- The risks that may threaten the achievement of the service organization's service commitments and system requirements, and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Schellman & Company, LLC

Irving, Texas
February 18, 2020

Section 2

Management's Assertion

MANAGEMENT'S ASSERTION

We have prepared the accompanying description of Planview's Spigit system, in Section 3, throughout the period March 16, 2019, to October 31, 2019, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Spigit system that may be useful when assessing the risks arising from interactions with Planview's system, particularly information about system controls that Planview has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security and availability ("applicable trust services criteria") set forth in TSP section 100, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Planview uses various subservice organizations for data center hosting, encrypted data backup storage, and embedded business reporting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Planview, to achieve Planview's service commitments and system requirements based on the applicable trust services criteria. The description presents Planview's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Planview's controls. The description does not disclose the actual controls at the subservice organizations.

We confirm, to the best of our knowledge and belief, that

a. the description presents Planview's Spigit system that was designed and implemented throughout the period March 16, 2019, to October 31, 2019, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period March 16, 2019, to October 31, 2019, to provide reasonable assurance that Planview's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Planview's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period March 16, 2019, to October 31, 2019, to provide reasonable assurance that Planview's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Planview's controls operated effectively throughout that period.

Section 3

Description of the System

Overview of Operations

Company Background

Planview, Inc. ("Planview" or the "Company") was founded in 1989 with a goal of providing comprehensive portfolio management solutions to enable better decision making and business accountability. Planview manages and operates Planview enterprise management software solutions via a Software as a Service ("SaaS") model.

This description specifically addresses the Spigit software product.

Description of Services Provided

Planview Spigit is an innovation management system that crowd sources and refines ideas into solutions to help customers solve complex business problems and manage the entire idea lifecycle, from idea to impact.

Planview Spigit enables organizations to capture ideas to solve business problems through the formation of challenges. These challenges permit users to submit ideas via a configurable form in real time. Ideas can incorporate images, text, links, and attachments where permitted by customers. Ideas can also be captured via anonymous or known usernames which is configured by the customers. Finally, Ideas can be posted through both desktop and mobile browser interfaces.

Principal Service Commitments and System Requirements

Planview designs its processes and procedures related to the in-scope system to meet its objectives for its Spigit system. Those objectives are based on the service commitments that Planview makes to user entities, the laws and regulations that govern the provision of the Spigit system, and the financial, operational, and compliance requirements that Planview has established for the services.

The security and availability commitments to user entities are documented and communicated in service level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. The principal security and availability commitments are standardized and include, the following:

- The system will be available at least 99.5% excluding maintenance and downtime
- Customer data is kept confidential and secured from unauthorized disclosure
- Logical access controls are in place to safeguard the receipt, storage, and internal transfer of customer data within the system boundaries, and limit access to customer data based on role
- Changes to the in-scope system will be managed to mitigate the risk of service disruption
- Risks are managed to limit the risks to service delivery to an acceptably low level on an ongoing basis

Planview establishes operational requirements that support the achievement of the principal service commitments, relevant laws and regulations, and other system requirements. Including the use of encryption technologies and logical access and authentication technologies to protect system user data both at rest and in transit; and the use of role-based access control to limit logical access privileges to authorized individual; and database management processes to ensure databases and supporting tables are loaded, maintained and monitored for completion and performance; and systems monitoring practices to ensure operations personnel are notified of conditions that threaten the stability and availability of the system; and system outages, when applicable, are reviewed for root causes and remediation process are implemented accordingly; and necessary system change management procedures to support the requisite authorization, documentation, testing, and approval of system changes.

Such requirements are communicated in Planview'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, trained, and managed. 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 Spigit system.

In accordance with our assertion, and the description criteria, the aforementioned service commitments and requirements are those principal service commitments and requirements common to the broad base of users of the system and may therefore not fully address the specific service commitments and requirements made to all system users, in each individual case.

Components of the System Used to Provide the Service

System Boundaries

A system is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of the system description is to delineate the boundaries of the system, which includes the services outlined above and the five components described below: infrastructure, software, people, procedures, and data.

Infrastructure and Software

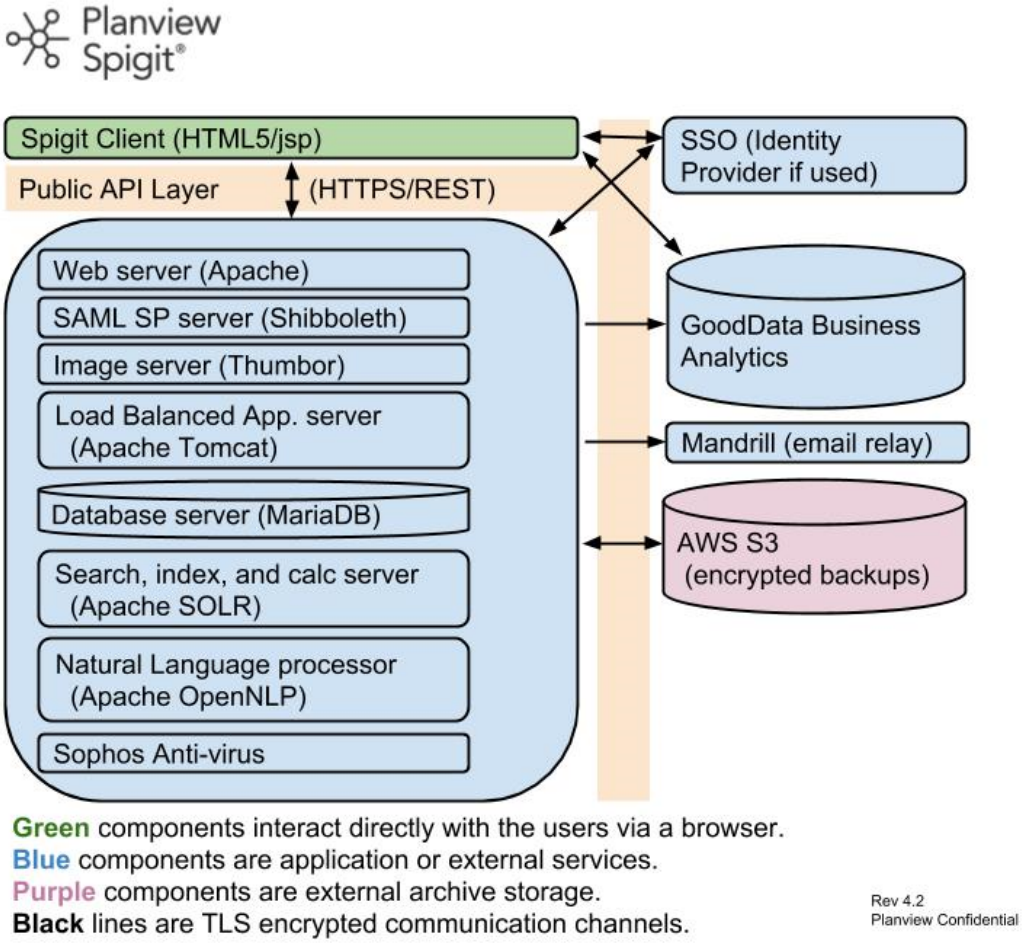
The Spigit system is hosted on dedicated Linux (CentOS) servers and network devices provided by Rackspace, Inc. ("Rackspace"), with data backups for disaster recovery hosted by Amazon Web Services ("AWS") Simple Storage Service ("S3") and reporting hosted by GoodData Corporation ("GoodData"). Planview uses Rackspace data centers to host Planview Spigit, which are located in the United States of America ("US"), United Kingdom ("UK"), Germany/Deutschland ("DE"), Hong Kong ("HK"), and Australia ("AU"); AWS S3 regions that are located in US, UK, DE, and AU; and GoodData data centers that are located in the US and UK. All data centers use the same architecture and technology. Planview Spigit customers select their data center location of choice, usually dictated by reducing network latency or meeting regulatory or internal policy requirements.

Customers are deployed on a dedicated application stack and dedicated database on either customer dedicated or customer shared servers. Each data center location uses shared network devices (e.g. switches and routers), System dedicated intrusion detection and intrusion prevention devices, System dedicated firewalls, and System dedicated servers and storage. All customer data is stored in encrypted storage.

Customers access Planview Spigit from the Internet via encrypted Hypertext Transfer Protocol Secure ("HTTPS") communication channels using Transport Layer Security ("TLS") with strong ciphers. Firewall rules are in place to restrict network access. Additional customer specific IP restriction is an option offered to customers to further restrict access to pre-authorized IP addresses or IP address ranges. All communications traffic between the customer and the data center is examined by actively monitored intrusion detection devices that can automatically respond to suspicious activity blocking further traffic or alerting security analysts when additional investigation is warranted. Planview Spigit's network is separate from Planview's network and requires virtual private network ("VPN") and multi-factor authentication to access.

The System is a HyperText Markup Language ("HTML") 5 and jsp customer browser-based application with the business processing logic executing on the data center housed servers. The browser client will sense the capabilities of the device hosting the users' browser, appropriately format the available display, and select the appropriate functions available to the device.

Spigit utilizes the following technology architecture to support the application:



The in-scope infrastructure consists of multiple applications, operating system platforms and databases, as shown in the table below:

Primary Infrastructure			
Production Application	**Business Function Description**	**Operating System Platform**	**Physical Location**
Apache Web	Apache Web server with security modules is utilized to manage secure active web sessions and serve user requested web pages, that may contain text, graphics, images, video, and other application data, and to service Representational State Transfer (“REST”) based application programming interface (“API”) requests. The web server proxies all traffic to the Apache Tomcat application server.	Linux CentOS	Rackspace Colocation Data Centers
Apache Tomcat	Apache Tomcat application servers are utilized in a load balanced configuration as the Java web application server.	Linux CentOS	
MariaDB	MariaDB is utilized as the database server and database replication server	Linux CentOS	
AWS S3	Amazon S3 storage is utilized for encrypted customer data backups that can be recovered in a disaster scenario at any alternate data center.	N/A	AWS data centers

People

Planview has a staff of approximately 700 individuals located in offices across North America and Europe organized in the following groups:

- Executive Management – responsible for overseeing company-wide activities, establishing, and accomplishing goals, and overseeing objectives.
- Security Steering Committee – comprised of key members in IT, Security, and Executive Management and responsible for security and availability related strategy, risk management, policies, and communication.
- Product Development – responsible for product development, product quality assurance (QA), product release management, and escalated product support.
- Cloud Operations ("CloudOps") – responsible for configuring, maintaining, monitoring, and upgrading the infrastructure and software including infrastructure management, server administration, storage management, application administration, database administration, delivery, and backup and recovery.
- Security Operations ("SecOps") – responsible for vulnerability management, vendor audit program, monitoring and compliance of security issues and incidents throughout the service delivery infrastructure.
- Corporate Information Technology ("IT") – responsible for workstation / laptop end point protection and maintaining the corporate infrastructure and supporting software.
- Human Resources (HR) – responsible for HR policies, practices, and processes with a focus on key HR department delivery areas (e.g. talent acquisitions, employee retention, compensation, employee benefits, performance management, employee relations and training, and development).
- Customer Care – responsible for providing customer support as first point of contact and application support.
- Customer Success – responsible for customer training, customer deployment, and customer innovation program strategy development and support.

Procedures

Access, Authentication and Authorization

Employees access Planview corporate network with an assigned valid Active Directory account and password. Minimum password requirements are enforced through parameters set in Active Directory. Users are also required to separately sign on to any systems or applications that do not use the shared sign-on functionality in Active Directory. Access to the production environment and internal tools is restricted to authorized personnel or on an as-needed basis. Resources are protected through the use of native system security and add-on software products that identify and authenticate users and validate access requests against the users' authorized roles, as specified in access control lists.

External users access the Planview Spigit application through the Internet on their web-browser using a valid user ID and password. Access to the application is secured using TLS encryption via HTTPS. The recommended best practice for authentication is to enable Single Sign On ("SSO") via SAML 2.0 integration and disable form-based authentication. Leveraging SSO integrates password policies and user management solution with the customer's identify provider. The application can also be configured for form-based authentication to enforce authentication parameters (e.g. minimum length, complexity, etc.) configured at the discretion of the customer. Customers are responsible for administrating access to their own environment by identifying appropriate employees to perform user account management including access approval, provisioning and deprovisioning. Planview does not provide external users with access to internal system components.

Internal access to the production environment including production operating systems, databases, application, and supporting infrastructure components is restricted to authorized Planview personnel via VPN access to the production network using an encrypted connection and valid operating system, database, application, or device user account. Connection to the VPN requires multi-factor authentication (MFA) through DUO. Disabling MFA access blocks the Planview personnel from accessing other system components. Access to Linux based

production operating systems and database is authenticated via the use of cryptographic keys (private/public) and communication sessions are encrypted with secure shell (SSH). Authorized system administration personnel are responsible for provisioning user access rights to the production environment.

Access Requests and Access Revocation

Newly hired employees are assigned a position in the HR management system. Prior to the employee's start date, the HR management system creates a report of employee user IDs to be created and the level of access to be granted within the corporate network. The report is used by Corporate IT to assign access rights. Access to the production systems are restricted to authorized personnel on an as-needed basis and requires additional documented approval from Operations management.

The HR department generates a ticket notifying members of the Corporate IT of employee terminations or contractors who no longer require access to the corporate network and production systems. Access to the corporate network and production systems is revoked as a part of the termination process.

Additionally, user access to the corporate network and productions systems is reviewed on at least semi-annual basis. Access flagged for modification or removal is tracked in a ticket and removed upon completion of the review. The review includes a comparison of the user access listings to the list of active employees and vendors to identify terminated users who no longer require access. The review also incorporates an assessment of access based on current job responsibilities to identify users who no longer require access to perform their job requirements.

Change Management

Planview has a formalized Change Management Policy addressing responsibilities and specific change requirements. The Spigit team follows an agile methodology in their software development life cycle (SDLC) process. Spigit source code is maintained in GitHub, a source code management system that provides collaboration features for bug tracking, feature requests, and task management. The SDLC is broken into two major components: 1) Define the feature or function, and 2) Develop the feature or function.

Definition Steps

- Define the feature to implement from the business perspective, or define the internal improvement such as improve performance or refactoring code to use best practices
- Identify the security and privacy requirements
- If procuring, complete third-party evaluation
- Prioritize features based on release calendar
- Detail the features into User Stories with acceptance criteria
- Create mockups for user interaction based on User Stories
- Perform security and availability feature review

Development Steps

- Create or update test scenarios
- Design features [App Developer]
- Perform architectural design review [Architecture team]
- Develop new features [App Developer]
- Develop unit tests [App Developer]
- Develop automated tests for the new scenarios [Automation engineer]
- Perform peer code reviews [App Developer]
- Trigger automated integration tests and code review using CI tools [App Developer]
- Perform code reviews for merging [App Developer / Architecture team]

- Execute manual and automated tests and send feedback to Development Team [QA]
- Security, availability, and confidentiality testing: Perform edge/boundary value condition testing and Drive tests with security, availability and confidentiality requirements and features [QA]
- Complete QA verification and validation

The product development team specifies the content of a product release and authorizes general release after successful completion of final testing, verification, and validation. Requests to move changes to production are evaluated to assess potential effects of the requested change on the security and availability of the system. Application changes require prior product development management approval for general release. All System changes require review, testing in a non-production environment, and hosting operations management approval before being moved into production. Development, test, staging, and production environments are logically segregated. Infrastructure changes are deployed to the staging environment and required to run successfully before they are authorized for production deployment.

Data Backup and Disaster Recovery

Planview maintains a business continuity plan and separate disaster recovery plans for each product that include the development of planned procedures and alternative processing solutions to respond to, mitigate, and recover from disrupted business operations. These plans are reviewed, updated, and tested on an annual basis, and any key learning is incorporated back into the plan.

The Planview Spigit customer data is fully backed up on a nightly basis to AWS S3 and retained for 30 days. A Zendesk ticket is automatically opened by the backup job to notify operations personnel of any backup failure.

Incident Response

Planview continuously monitors for incidents reported by third-party monitoring tools, employees, and customers. Security events requiring investigation are tracked in a help desk ticket and monitored until resolved. Procedures for internal reporting of security failures, incidents, and concerns are described in the Acceptable Use Terms provided to all employees. Employees are instructed to report potential security incidents or breaches to the internal help desk, which is consistently monitored by members of the IT team who risk rank reported incidents and reassign incidents to the Security Operations Engineers as necessary for remediation.

Planview provides customers with a support site that contains system documentation and access to report incidents. Customer incidents are documented and resolved in accordance with the Service Level Agreement (“SLA”) per the contract with the customer.

System Monitoring

Several automated monitoring tools are leveraged by Planview to identify security events and performance issues, including Nagios, UpTrends, and Rackspace monitoring. Events identified through the varying monitoring tools are documented, reviewed, and resolved in accordance with the incident management process.

Nagios is used by Planview to monitor the performance and availability of systems. Metrics being monitored include CPU utilization, system load, disk usage, and overall application health. Nagios is configured to send an alert automatically if a predefined threshold has been met or exceeded.

Uptrends is used to monitor uptime of external facing endpoints and to test customer instances for response time.

Rackspace automatically monitors the server and network health as part of the third-party hosting agreement with Planview.

Data

Data includes information entered by the customers’ users, and information generated through user actions in the system. Data may also include logs, metadata, navigation data, and data backups. Data is stored in a manner that separates each customer’s data from other customers. Customer data is managed, processed, and stored in accordance with relevant data protection regulations with specific requirements formally established in customer contracts. All user-generated content in the Planview environment is owned solely by the user.

Elements of personally identifiable information stored and processed by Planview Spigit include User identification ("ID"), name, surname, e-mail address, internet protocol ("IP") address, user role, and other information the users add to their profile. Planview Spigit also stores and processes information about ideas, including idea description, supporting documents, idea comments, idea votes, idea rankings, and related information needed to manage an innovation program.

Significant Changes During the Review Period

There were no significant changes that are likely to affect report users' understanding of how the in scope system is used to provide the services covered by this examination during the period.

Subservice Organizations

The data center hosting service provided by Rackspace, encrypted data backup storage provided by AWS, and embedded business reporting service provided by GoodData were not included within the scope of this examination.

The following table presents the applicable Trust Services criteria that are intended to be met by controls at Rackspace, AWS, and GoodData, alone or in combination with controls at Planview, and the types of controls expected to be implemented at Rackspace, AWS, and GoodData to achieve Planview's service commitments and system requirements based on the applicable trust services criteria.

Control Activity Expected to be Implemented by Rackspace, AWS, and GoodData	Applicable Trust Services Criteria
AWS and Rackspace are responsible for managing logical access to the underlying network, virtualization management, and storage devices for the encrypted backup storage and cloud hosting services where the Planview systems reside.	CC6.1-3, and CC6.5
AWS, Rackspace and GoodData are responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.	CC6.4-5
AWS, Rackspace and GoodData are responsible for monitoring physical access to the data center facilities that house the production backup media, and other system components such as firewalls, routers, and servers.	CC7.2
AWS, Rackspace and GoodData are responsible for ensuring the data center facilities are equipped with environmental security safeguards.	A1.2

CONTROL ENVIRONMENT

The control environment at Planview is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by the Security Steering Committee and operations management.

Integrity and Ethical Values

Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of key processes. Planview's Security Steering Committee and management recognize their responsibility to foster a strong ethical environment within the Company to ensure that its business affairs are

conducted with integrity and in accordance with high standards of personal and corporate conduct. This responsibility is reflected in the Company Ethics section of the Employee Handbook, which is distributed to all employees of the organization.

Employees are required to maintain ongoing compliance with all Planview policies, the Employee Handbook, and with lawful and ethical business practices. Each employee is required to affirm that they have received, read, understood, and plan to comply with the requirements in the Employee Handbook upon employment with the Company. Planview policies include sanctions for employee misconduct or noncompliance with policies.

Security Steering Committee Oversight

The Planview Security Steering Committee is comprised of key members in IT, security, and executive management and is responsible for security and availability related strategy, risk management, policies, and communication.

The Security Steering Committee is responsible for overseeing Planview's corporate governance and has discretion to delegate a broad range of powers and decisions to manage the entity. The Security Steering Committee members oversee the activities of Planview's functional groups and takes action with respect to its security and availability controls and responsibilities as recommended by the Security team leadership. The Security Steering Committee meets on a quarterly basis or more frequently, if necessary. Security Steering Committee meetings include a review and evaluation of operating performance, strategy, and corporate governance.

Organizational Structure and Assignment of Authority and Responsibility

Planview's organizational structure provides the framework within which its activities for achieving entity wide objectives are planned, executed, controlled, and monitored. Planview has established an organizational structure that includes consideration of key areas of authority and responsibility, as well as appropriate lines of reporting. A Planview Organization Chart is maintained and available to all employees.

Formal written job descriptions are developed and maintained for positions that access or impact key systems, including Developers and Operations team members. Job descriptions include specific responsibilities and professional and academic requirements. Changes to formal written job descriptions are submitted to HR for review and approval.

Commitment to Competence

Managers within the respective functional groups of the organization determine the need for additional resources and submit formal job requisitions to senior management for approval. Once requisitions have been approved by the appropriate individuals, HR begins sourcing and recruiting for the available position. HR screens potential candidates based on job experience and academic accomplishments and sends selected résumés to respective managers for review. The managers review documentation and select candidates for interviews which are scheduled by HR and conducted by the manager.

Job descriptions are referenced during the recruiting and hiring process to confirm that new employees meet academic and professional requirements and exhibit sufficient competence to perform key job responsibilities. Individuals offered a position at Planview are subject to background checks prior to commencing employment, as appropriate for each country with respect to local laws and regulations. Background checks include substantiation of education, previous employment, and criminal record, as applicable. HR also requests employment references to further evaluate employee experience and competence.

Employees receive onboarding information including an overview of Planview's HR policies and procedures, an offer letter or employment contract, Employee Handbook, Information Security policy, and relevant compensation materials. Employees acknowledge receipt and review of the Employee Handbook and Company policies and procedures during onboarding. Employees, contractors, partners, and service providers acknowledge and sign a Confidentiality Agreement / Non-Disclosure Agreement prior to engagement or employment.

Planview has established formal classroom, web-based, and on-the-job employee training programs for critical departments and functions. Programs include orientation on the basics of the functional team's operations, individualized instruction manuals for selected departments, and regularly scheduled department workshops. Employees are also encouraged to actively participate in professional organizations and forums to maintain their knowledge and develop awareness of issues facing Planview and its customers.

Accountability

A security steering committee is in place and meets on a quarterly basis to identify and discuss risk, security, and privacy concerns. Management weighs each risk prior to determining the course of action for the identified risk. Organizational policies are in place to address the hiring process, new hire orientation, periodic evaluations, counseling, promotions, compensation, and remedial actions for violations of established policies.

Employee performance is reviewed continuously through management oversight. Performance improvement plans are developed and communicated for employees who do not consistently meet job requirements. Employees are also continuously assessed for adherence to standards of conduct and compliance with internal regulations. Violations of Company policies result in disciplinary action, including sanctions if considered appropriate.

Risk Assessment

The process of identifying, assessing, and managing risks is a critical component of Planview's internal control system. Planview regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security and availability. The information security team assesses security risks on an ongoing basis through regular leadership meetings, review of security event logs, and vulnerability assessments. Planview management also monitors controls to consider operation of controls as intended and whether controls are modified as appropriate for changes in conditions or risks facing the organization.

Objective Setting

The principal service commitments and system requirements form the objectives of the Planview services within scope. Customer commitments relating to security and availability are outlined in SLAs included in customer contracts. Management formally documents the company's service commitments and related requirements to ensure these commitments are met in the design and operation of internal controls. These objectives are utilized in the Planview risk assessment and risk mitigation processes.

Risk Identification, Analysis and Mitigation

An informal risk assessment is performed on an ongoing basis and the results are reviewed by the Security Steering Committee. A formal risk assessment is performed, at a minimum, annually. Results of the assessment are communicated to the Security Steering Committee and documented in the Planview risk register. Attendees include the Head of Information Security and senior management from business units throughout the Planview organization.

The risk assessment process includes identifying the risk then documenting the risk relevant details for analysis. Risks are evaluated based on both the likelihood they would occur and the impact to the organization if they did occur. This evaluation forms the overall risk score and is documented in the risk register for each risk. The Steering Committee has a documented risk management strategy which includes risk avoidance, risk acceptance, risk sharing, and risk reduction.

Risk avoidance and reduction strategies require a risk treatment plan to be formally developed and implemented to reduce the related risk to an acceptably low level. Management formulates a risk treatment plan that

documents risk treatment decisions including designed control activities to mitigate risks to defined risk tolerance levels as a result of the annual risk assessment process. All risk acceptance strategies require Security Steering Committee approval.

As part of the risk assessment process, management and IT discuss recent events, the state of the Company's systems, upcoming changes, and any security issues or concerns. Internal control evaluations are also incorporated into the risk management process. Additionally, management discusses and manages risks related to the potential for fraud, the identification and assessment of risks that may affect system's security and availability commitments, and risks that may arise from business disruptions. Deficiencies are documented in the Risk Register and remediation plans are defined. Risks are then monitored on an ongoing basis to account for changes in the control environment.

Risks affecting the organization and recommended courses of action are also identified and discussed during weekly meetings between Management and the SecOps group. Senior management considers developments in technology and the impact of applicable laws and regulations on Planview's security posture. Changes in security threats and risks identified during the weekly meetings are reviewed and updates to existing control activities and information security policies are performed as necessary.

Risks are documented in the Planview risk register. Documentation includes, at a minimum, the following:

- Risk Owner
- Description of Risk
- Probability
- Impact
- Criticality (Probability x Impact)
- Status

Risks contained in the risk register are communicated periodically with the Security Steering Committee and necessary stakeholders.

The information security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by management.

Risk Factors

Management considers risks that can arise from both external and internal factors including the following:

External Factors

- Technological developments
- Changing customer needs or expectations
- Competition that could alter marketing or service activities
- New legislation and regulation that could force changes in policies and strategies
- Natural catastrophes that could lead to changes in operations or information systems
- Economic changes that could have an impact on management decisions

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud
- Fraud incentives and pressures for employees
- Fraud opportunities

- Employee attitudes and rationalizations for fraud
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers fraud as a component of its ongoing risk management processes. While the fraud risk considerations are not documented in writing, fraud considerations are discussed with members of the Security Steering Committee during the annual risk assessment and periodically as risk assessment activities are performed.

TRUST SERVICES CRITERIA AND RELATED CONTROL ACTIVITIES

Integration with Risk Assessment

Along with assessing risks, management has identified and put into effect actions needed to address those risks. In order to address risks, control activities have been placed into operation to help ensure that the actions are carried out properly and efficiently. Control activities serve as mechanisms for managing the achievement of the security and availability categories.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section 4 of this report to eliminate the redundancy that would result from listing the items in this section and repeating them in Section 4. Although the applicable trust criteria and related control activities are included in Section 4, they are, nevertheless, an integral part of Planview's description of the system.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section 4, the Testing Matrices, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Trust Services Criteria Not Applicable to the In-Scope System

The Trust Services criterion presented below, is not applicable to the Spigit system within the scope of this examination. As a result, an associated control is not required to be in place at the service organization for the omitted applicable trust services criterion. The following table presents the trust services criterion that is not applicable for the Spigit system at Planview. The not applicable trust services criterion is also described within Section 4.

Criteria #	Reason for Omitted Criteria
CC1.2	Not applicable. An independent board of directors is not required or utilized for the in-scope system or to achieve the system's objectives. Planview has implemented a Security Steering Committee comprised of Planview management to perform the relevant oversight functions.

Information and Communication Systems

Information and communication is an integral component of Planview's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. Third-party data collection and monitoring tools are leveraged to compile data relating to system performance and availability, security, and incidents. These tools automate the data collection process to limit manual error and improve data quality. Data obtained through third-party sources, in combination with customer-reported and employee-reported data, are reviewed on an on-going basis by IT and management to support timely and appropriate decision-making and communication.

Internal Communications

The Company has implemented various methods of communication to help employees understand their individual roles and responsibilities, gain sufficient knowledge of the system and its components, and become aware of system changes. These include documented policies and procedures, formal and informal training programs, and the use of e-mail and real-time messaging applications to communicate time-sensitive information. System descriptions are available to internal users that describe significant system components as well as the purpose and design of the system. Additionally, a process is in place to communicate system changes affecting internal users prior to implementation.

External Communications

Planview is also responsible for communicating relevant information to customers, including the system description, incident reporting procedures, system changes, and breaches of information. System descriptions that detail significant system components as well as the purpose and design of the system are available to external users on the Planview website. In the unlikely incident of a breach of sensitive information, procedures are in place to communicate the breach to the affected parties in compliance with government regulation and company policy. There were no consequential incidents or security breaches identified or reported during the reporting period.

Monitoring

Monitoring is a process that assesses the quality of internal control performance over time. It involves assessing the design and operation of controls and taking necessary corrective actions. This process is accomplished through ongoing activities, separate evaluation, or a combination of the two. Monitoring activities also include using information from communications from external parties such as user entity complaints and regulatory comments that may indicate problems or highlight areas in need of improvement. Management has implemented monitoring practices to assess and evaluate the performance of controls over time.

Ongoing Monitoring

Planview performs ongoing monitoring to help ensure that business systems operate effectively on a continuous basis. Aspects of the ongoing monitoring procedures include the following:

- The Security Steering Committee, led by the head of information security and comprised of key leaders from organizations throughout the company, meets quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.
- The SecOps team uses third-party software to perform vulnerability scans at least quarterly and contracts with a third-party vendor to perform penetration testing at least annually to measure the security posture of a target system or environment
- The SecOps team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations.
- Monitoring applications are utilized to monitor and analyze the in-scope systems for possible or actual security breaches and system availability incidents.

Planview places a great degree of emphasis around ongoing monitoring activities to ensure the control environment is functioning as intended. Planview performs daily oversight over the alerts and reports from monitoring and assessment tools and utilizes a tracking system to track system vulnerabilities and potential security and availability incidents. Any deficiencies to the effectiveness of these monitoring activities would result in remediation plans that are monitored until resolution.

Separate Evaluations

Management has implemented an internal audit program to evaluate the performance of specific control activities and processes over time and confirm that the in-scope controls were consistently applied as designed and operating effectively.

Subservice Organization Monitoring

A Vendor Management Program is in place to facilitate vendor selection, review, and ongoing vendor management to mitigate risks to security or availability.

Non-Disclosure Agreements and Services Agreements with defined terms, conditions, and responsibilities are established with third parties who have a potential impact to the system or access sensitive data. Confidentiality clauses are incorporated in service agreements, which are signed by both parties prior to contracting. Management is also responsible for ensuring business associate agreements are current for third parties as part of the Vendor Management program.

Planview relies on cloud-based solutions and external service providers for various aspects of the Spigit system as detailed in “Subservice Organizations” section of this report. Planview performs a review of subservice organizations' attestation reports (e.g. SOC 2®, ISO 27001, etc.) on an annual basis to verify if the subservice organization has controls in place to address Planview’s security and availability requirements and whether they were operating effectively within the period. Management evaluates if the reports have any exceptions noted and if the exceptions will impact the Planview system. Management also verifies if any user entity controls required by subservice organizations are appropriately addressed at Planview.

Evaluating and Communicating Deficiencies

Planview management assess results of ongoing system operations using periodic internal reporting and reviews. Deficiencies identified are communicated to personnel responsible for taking corrective action. Corrective action is monitored to ensure it attains the expected results.

COMPLEMENTARY CONTROLS AT USER ENTITIES

Complementary user entity controls are not required, or significant, to achieve the service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the Spigit system provided by Planview. The scope of the testing was restricted to the Spigit system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period March 16, 2019, to October 31, 2019.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable trust services criteria were achieved during the review period. In selecting the tests of controls, Schellman considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Observation	Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g. resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g. approvals, authorizations, etc.).

Sampling

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Schellman utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Schellman, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than the aforementioned, constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the operating effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the applicable trust services criteria are presented in the "Subservice Organizations" section within Section 3.

SECURITY CATEGORY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity's security policies.	Inquired of the HR operations analyst regarding employee security awareness training to determine that employees were required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity's security policies.	No exceptions noted.
		Inspected evidence of employee security awareness training completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of employee security awareness training completion for a sample of current employees to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
CC1.1.2	Educational and background checks are performed for employees as a component of the hiring process.	Inspected evidence of educational and background checks for a sample of employees hired during the review period to determine that educational and criminal background checks were performed for each employee sampled.	The test of the control activity disclosed that educational and criminal background checks were not evidenced for one of 25 employees sampled.
CC1.1.3	Employees are required to sign an acknowledgment form upon hire indicating that they have been given access to the employee handbook and understand their responsibilities for compliance to ethical standards outlined in the employee handbook.	Inquired of the HR operations analyst regarding the completion of acknowledgement forms upon hire to determine that employees had been given access to the employee handbook and that they understood their responsibilities for compliance to ethical standards outlined in the employee handbook.	No exceptions noted.
		Inspected the employee handbook and the signed acknowledgement forms for a sample of employees hired during the review period to determine that an acknowledgement form was signed for each employee sampled.	No exceptions noted.
CC1.1.4	Employees, consultants, and third-party vendors agree to non-disclosure agreements prior to engagement or employment.	Inquired of HR operations analyst regarding the use of non-disclosure agreements for employees, consultants, and third-party vendors to determine that employees, consultants, and third-party vendors agreed to non-disclosure agreements prior to engagement or employment.	No exceptions noted.
		Inspected evidence of non-disclosure agreement completion prior to employment for a sample of employees, consultants, and third-party vendors hired during the review period to determine that non-disclosure agreements were completed prior to employment for each employee sampled.	No exceptions noted.
CC1.1.5	The disciplinary actions for employee misconduct or policy non-compliance are documented.	Inspected the employee handbook to determine that disciplinary actions for employee misconduct or policy non-compliance were documented.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
	Not applicable. An independent board of directors is not required or utilized for the in-scope system or to achieve the system's objectives. Planview has implemented a Security Steering Committee comprised of Planview management to perform the relevant oversight functions.		
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	Documented policies are in place and communicated to internal personnel via the company intranet to guide personnel in the entity's security and availability commitments. Management reviews and approves policies at least annually.	Inspected the information security policy documentation to determine that documented policies were in place regarding the entity's security and availability commitments.	No exceptions noted.
		Inspected the information security policy documentation approval documentation and evidence of communication to determine that the documented policies were communicated to internal personnel via the company intranet and reviewed and approved during the review period.	No exceptions noted.
CC1.3.2	Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system.	Inspected evidence of job descriptions for a sample of employment positions to determine that job descriptions were defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system for each employment position sampled.	The test of the control activity disclosed that defined job descriptions were not evidenced for four of 25 job descriptions sampled.
CC1.3.3	The organizational structure and reporting lines are defined in organizational charts, which are updated on an as-needed basis.	Inquired of the governance risk and compliance analyst regarding organizational structure to determine that organizational charts were in place and updated on an as-needed basis.	No exceptions noted.
		Inspected the company organizational charts to determine that organizational charts were in place and reporting lines were defined in organizational charts, and that charts were updated on an as-needed basis.	No exceptions noted.
CC1.3.4	Employees, consultants, and third-party vendors agree to non-disclosure agreements prior to engagement or employment.	Inquired of HR operations analyst regarding the use of non-disclosure agreements for employees, consultants, and third-party vendors to determine that employees, consultants, and third-party vendors agreed to non-disclosure agreements prior to engagement or employment.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of non-disclosure agreement completion prior to employment for a sample of employees, consultants, and third-party vendors hired during the review period to determine that non-disclosure agreements were completed prior to employment for each employee sampled.	No exceptions noted.
CC1.3.5	The security steering committee, led by the head of information security and comprised of key leaders from organizations throughout the company, meets quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.	Inquired of the governance risk and compliance analyst regarding the security steering committee to determine that the security steering committee met quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.
		Inspected the listing of security steering committee members to determine that the security steering committee was comprised of key leaders from organizations throughout the company.	No exceptions noted.
		Inspected evidence of security steering committee meetings for a sample of quarters during the review period to determine that the security steering committee met to discuss organizational risk, security and privacy concerns, and areas of focus for each quarter sampled.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity's security policies.	Inquired of the HR operations analyst regarding employee security awareness training to determine that employees were required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity’s security policies.	No exceptions noted.
		Inspected evidence of employee security awareness training completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of employee security awareness training completion for a sample of current employees to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
CC1.4.2	Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system.	Inspected evidence of job descriptions for a sample of employment positions to determine that job descriptions were defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system for each employment position sampled.	Refer to the test results for control activity CC1.3.2.
CC1.4.3	Educational and background checks are performed for employees as a component of the hiring process.	Inspected evidence of educational and background checks for a sample of employees hired during the review period to determine that educational and criminal background checks were performed for each employee sampled.	Refer to the test results for control activity CC1.1.2.
CC1.4.4	Developers are required to complete secure development training on an annual basis.	Inquired of the governance and risk compliance analyst regarding secure development training to determine that developers were required to complete secure development training on an annual basis.	No exceptions noted.
		Inspected evidence from the learning management system to determine that developers were required to complete secure development training on an annual basis.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system.	Inspected evidence of job descriptions for a sample of employment positions to determine that job descriptions were defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system for each employment position sampled.	Refer to the test results for control activity CC1.3.2.
CC1.5.2	The organizational structure and reporting lines are defined in organizational charts, which are updated on an as-needed basis.	Inquired of the governance risk and compliance analyst regarding organizational structure to determine that organizational charts were in place and updated on an as-needed basis.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the company organizational charts to determine that organizational charts were in place and reporting lines were defined in organizational charts, and that charts were updated on an as-needed basis.	No exceptions noted.
CC1.5.3	The disciplinary actions for employee misconduct or policy non-compliance are documented.	Inspected the employee handbook to determine that disciplinary actions for employee misconduct or policy non-compliance were documented.	No exceptions noted.
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.			
CC2.1.1	Documented policies are in place and communicated to internal personnel via the company intranet to guide personnel in the entity's security and availability commitments. Management reviews and approves policies at least annually.	Inspected the information security policy documentation to determine that documented policies were in place regarding the entity's security and availability commitments.	No exceptions noted.
		Inspected the information security policy documentation approval documentation and evidence of communication to determine that the documented policies were communicated to internal personnel via the company intranet and reviewed and approved during the review period.	No exceptions noted.
CC2.1.2	The CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	Inspected evidence of monthly system performance meetings and noted that the CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	No exceptions noted.
CC.2.1.3	Penetration testing is performed on an annual basis by a third-party vendor. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of penetration testing completed by a third-party vendor to determine that identified critical and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
CC.2.1.4	Vulnerability scans are performed on an at least quarterly basis. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of vulnerability scan completion and scan tool configurations to determine that vulnerability scans are completed on at least a quarterly basis and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC.2.1.5	Enterprise monitoring applications are configured to monitor the in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	Inspected evidence of enterprise monitoring application configurations and example alert to determine that enterprise monitoring applications are configured to monitor in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	No exceptions noted.
CC.2.1.6	Internal audits are performed on an at least annual basis by the compliance team. The audit results are documented and reviewed by management.	Inquired of the governance risk and compliance analyst to regarding internal audit to determine that internal audits are performed on at least an annual basis by the compliance team and the results are documented and reviewed by management.	No exceptions noted.
		Inspected evidence of internal audits performance to determine that internal audits are performed on at least an annual basis by the compliance team and that results are documented and reviewed by management.	No exceptions noted.
CC.2.1.7	The information security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by management.	Inquired of the governance risk and compliance analyst regarding emerging technology and changes to applicable law or regulations to determine that the information security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by management.	No exceptions noted.
		Inspected evidence of the information security team's monitoring of emerging technologies to determine that the information security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations are considered by management.	No exceptions noted.
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.			
CC2.2.1	Documented policies are in place and communicated to internal personnel via the company intranet to guide personnel in the entity's security and availability commitments. Management reviews and approves policies at least annually.	Inspected the information security policy documentation to determine that documented policies were in place regarding the entity's security and availability commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security policy documentation approval documentation and evidence of communication to determine that the documented policies were communicated to internal personnel via the company intranet and reviewed and approved during the review period.	No exceptions noted.
CC2.2.2	Employees are required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity's security policies.	Inquired of the HR operations analyst regarding employee security awareness training to determine that employees were required to complete security awareness training upon hire and on an annual basis thereafter to understand their obligations and responsibilities to comply with the entity's security policies.	No exceptions noted.
		Inspected evidence of employee security awareness training completion for a sample of employees hired during the review period to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
		Inspected evidence of employee security awareness training completion for a sample of current employees to determine that security awareness training was completed for each employee sampled.	No exceptions noted.
CC.2.2.3	Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system.	Inspected evidence of job descriptions for a sample of employment descriptions to determine that Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system for each employment description sampled.	Refer to the test results for control activity CC1.3.2.
CC.2.2.4	Documented incident response policy is communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	Inquired of governance and risk compliance analyst regarding the incident response policy to determine that the incident response policy was documented and communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the incident response policy to determine that the incident response policy was documented and communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	Information regarding the design and operation of the system and its boundaries and the entity's security and availability principal service commitments and the associated system requirements are documented and communicated to external users via public website, customer contracts or service level agreements.	Inquired of the governance risk and compliance analyst regarding information related to the design of the system and its boundaries and the entity's security and availability principal service commitments and the associated system requirements to determine that the entity's security and availability principles service commitments are documented and communicated to external users via public website, customer contracts or service level agreements.	No exceptions noted.
		Inspected the public website to determine that information regarding the design and operation of the system and its boundaries and the entity's security and availability principal service commitments and the associated system requirements are documented and communicated to external users.	No exceptions noted.
CC2.3.2	Changes to the system that may affect system security or availability are communicated to customers via system alerts and/or release note via customer-facing website.	Inspected example release notes to determine that changes to the system that may affect system security or availability are communicated to customers via system alerts and/or release note via customer-facing website.	No exceptions noted.
CC2.3.3	Employees, consultants, and third-party vendors agree to non-disclosure agreements prior to engagement or employment.	Inspected evidence of non-disclosure agreement completion prior to employment for a sample employees, consultants, and third-party vendors hired during the review period to determine that non-disclosure agreements were completed prior to employment for each employee sampled.	No exceptions noted.
CC2.3.4	A support site is accessible by customers to report security incidents, concerns, and complaints.	Inspected the support site to determine that the support site is accessible by customers to report security incidents, concerns, and complaints.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.0: Risk Management and Design and Implementation of Controls			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Management formally documents the company's service commitments and related requirements to ensure these commitments are met in the design and operation of internal controls.	Inquired of the director of information security regarding the company's service commitments and related requirements to determine that those commitments and requirements were documented to ensure that they were met in the design and operation of internal controls.	No exceptions noted.
		Inspected the listing of principal service commitments and requirements to determine that Management formally documents the company's service commitments and related requirements.	No exceptions noted.
CC3.1.2	A risk assessment is performed on an annual basis that considers the following: • Potential for fraud • The identification and assessment of risks that may affect system's security and availability commitments • The risks that may arise from business disruptions. • Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inquired of the director of information security regarding the risk assessment process to determine that the risk assessment considered the potential for fraud.	No exceptions noted.
		Inspected the risk assessment documentation completed during the review period to determine that a risk assessment was completed during the review period and demonstrated the following: • Identified and assessed the risks that may affect system's security and availability commitments • Considered the risks that may arise from business disruptions • Identified risks were rated using a risk evaluation process • Risks were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC3.1.3	The security steering committee, led by the head of information security and comprised of key leaders from organizations throughout the company, meets quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.	Inquired of the director of information security regarding the security steering committee to determine that the security steering committee was led by the head of information security and comprised of key leaders to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the listing of security steering committee members to determine that the security steering committee was comprised of key leaders from organizations throughout the company.	No exceptions noted.
		Inspected the security steering committee agenda and meeting details for a sample quarter during the review period to determine that the security steering committee met during the quarter sampled to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.
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.			
CC3.2.1	A risk assessment is performed on an annual basis that considers the following: • Potential for fraud • The identification and assessment of risks that may affect system's security and availability commitments • The risks that may arise from business disruptions. • Identified risks are rated using a risk evaluation process and are formally documented, with mitigation strategies, for management review.	Inquired of the director of information security regarding the risk assessment process to determine that the risk assessment considered the potential for fraud.	No exceptions noted.
		Inspected the risk assessment documentation completed during the review period to determine that a risk assessment was completed during the review period and demonstrated the following: • Identified and assessed the risks that may affect system's security and availability commitments • Considered the risks that may arise from business disruptions • Identified risks were rated using a risk evaluation process • Risks were formally documented, with mitigation strategies, for management review.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	A risk assessment is performed on an annual basis that considers the potential for fraud.	Inquired of the director of information security regarding the risk assessment process to determine that the risk assessment considered the potential for fraud.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the risk assessment documentation completed during the review period to determine that a risk assessment was completed during the review period.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The information security team monitors the security impact of emerging technologies and the impact of changes to applicable laws or regulations is considered by management.	Inquired of the director of information security regarding the process for monitoring emerging technologies and legal and regulatory changes to determine that the information security team monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations was considered by management.	No exceptions noted.
		Observed the security monitoring process and inspected evidence of internal communication during the review period to determine that information security team monitored the security impact of emerging technologies and the impact of changes to applicable laws or regulations.	No exceptions noted.
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.			
CC4.1.1	The CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	Inspected evidence of monthly system performance meetings and noted that the CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	No exceptions noted.
CC4.1.2	Penetration testing is performed on an annual basis by a third-party vendor. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of penetration testing completed by a third-party vendor to determine that identified critical and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
CC4.1.3	Vulnerability scans are performed on an at least quarterly basis. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of vulnerability scan completion and scan tool configurations to determine that vulnerability scans are completed on at least a quarterly basis and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.1.4	Enterprise monitoring applications are configured to monitor the in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	Inspected evidence of enterprise monitoring application configurations and example alert to determine that enterprise monitoring applications are configured to monitor in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	No exceptions noted.
CC4.1.5	Internal audits are performed on an at least annual basis by the compliance team. The audit results are documented and reviewed by management.	Inquired of the governance risk and compliance analyst to regarding internal audit to determine that internal audits are performed on at least an annual basis by the compliance team and the results are documented and reviewed by management.	No exceptions noted.
		Inspected evidence of internal audits performance to determine that internal audits are performed on at least an annual basis by the compliance team and that results are documented and reviewed by management.	No exceptions noted.
CC4.1.6	Management reviews audit reports from third-party service providers on an annual basis and evaluates subservice organization controls and user-entity controls considerations to help ensure compliance with security and availability commitments and system requirements.	Inspected evidence of management review of audit reports for a sample of third-party service providers to determine that management review the audit reports of each third-party service provider sampled.	No exceptions noted.
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.			
CC4.2.1	The CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	Inspected evidence of monthly system performance meetings and noted that the CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	No exceptions noted.
CC4.2.2	Internal audits are performed on an at least annual basis by the compliance team. The audit results are documented and reviewed by management.	Inquired of the governance risk and compliance analyst to regarding internal audit to determine that internal audits are performed on at least an annual basis by the compliance team and the results are documented and reviewed by management.	No exceptions noted.
		Inspected evidence of internal audits performance to determine that internal audits are performed on at least an annual basis by the compliance team and that results are documented and reviewed by management.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2.3	The security steering committee, led by the head of information security and comprised of key leaders from organizations throughout the company, meets quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.	Inquired of the director of information security regarding the security steering committee to determine that the security steering committee was led by the head of information security and comprised of key leaders to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.
		Inspected the listing of security steering committee members to determine that the security steering committee was comprised of key leaders from organizations throughout the company.	No exceptions noted.
		Inspected the security steering committee agenda and meeting details for a sample quarter during the review period to determine that the security steering committee met during the quarter sampled to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.
CC4.2.4	Penetration testing is performed on an annual basis by a third-party vendor. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of penetration testing completed by a third-party vendor to determine that identified critical and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
CC4.2.5	Vulnerability scans are performed on an at least quarterly basis. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of vulnerability scan completion and scan tool configurations to determine that vulnerability scans are completed on at least a quarterly basis and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
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.			
CC5.1.1	The security steering committee, led by the head of information security and comprised of key leaders from organizations throughout the company, meets quarterly to discuss organizational risk, security and privacy concerns, and areas of focus.	Inquired of the director of information security regarding the security steering committee to determine that the security steering committee was led by the head of information security and comprised of key leaders to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the listing of security steering committee members to determine that the security steering committee was comprised of key leaders from organizations throughout the company.	No exceptions noted.
		Inspected the security steering committee agenda and meeting details for a sample quarter during the review period to determine that the security steering committee met during the quarter sampled to discuss organizational risk, security and privacy concerns, and areas of focus.	No exceptions noted.
CC5.1.2	Management formulates a risk treatment plan that documents risk treatment decisions including designed control activities to mitigate risks to defined risk tolerance levels as a result of the annual risk assessment process.	Inspected the risk treatment documentation to determine that risk treatment decisions including designed control activities to mitigate risks to defined risk tolerance levels as a result of the annual risk assessment process were documented within a risk treatment plan.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Control activities over technology are identified as part of the annual risk assessment process to support the achievement of objectives and are documented within the risk assessment report.	Inquired of the director of information security regarding the risk assessment process to determine control activities over technology were identified as part of the annual risk assessment process to support the achievement of objectives and were documented within the risk assessment report.	No exceptions noted.
		Inspected the risk assessment report to determine that control activities over technology were identified as part of the annual risk assessment process to support the achievement of objectives and were documented within the risk assessment report.	No exceptions noted.
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.			
CC5.3.1	Documented policies are in place and communicated to internal personnel via the company intranet to guide personnel in the entity's security and availability commitments. Management reviews and approves policies at least annually.	Inspected the information security policy documentation to determine that documented policies were in place regarding the entity's security and availability commitments.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the information security policy documentation approval documentation and evidence of communication to determine that the documented policies were communicated to internal personnel via the company intranet and reviewed and approved during the review period.	No exceptions noted.
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.			
CC6.1.1	Customer data is segregated through the use of application security controls that restrict customers to access their own data.	Inspected the application security control configurations to determine that customer data was segregated through the use of application security controls that restricted customers to access their own data.	No exceptions noted.
CC6.1.2	The in-scope systems are configured to authenticate internal users with a unique user account and enforce minimum password requirements or SSH public key authentication.	Inspected the user account listings and authentication configurations for a sample of in-scope systems to determine that each in-scope system sampled was configured to authenticate internal users with a unique user account and enforce minimum password requirements or SSH public key authentication.	No exceptions noted.
CC6.1.3	Planview provides customers with guidelines for secure authentication methods for Planview products.	Inspected the secure authentication methods guidelines to determine that Planview provided customers with guidelines for secure authentication methods for Planview products.	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts for employees who require access and are authorized for such.	Inspected the administrative user listings for a sample of in-scope systems with the assistance of senior manager of hosting operations to determine that administrative access privileges to each in-scope system sampled were restricted to user accounts for employees who required access and were authorized for such.	No exceptions noted.
	AWS and Rackspace are responsible for managing logical access to the underlying network, virtualization management, and storage devices for the encrypted backup storage and cloud hosting services where the Planview systems reside.		

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.2.1	Internal user access requests to the in-scope systems are documented and require the approval of IT Management.	Inspected the access approval documentation for a sample of users provided access during the review period to determine that internal user access requests to the in-scope systems were documented and approved by IT Management for each user sampled.	No exceptions noted.
CC6.2.2	Upon termination of an employee or a contractor, access to in-scope systems is revoked unless appropriate approval is obtained to extend access.	Inspected a listing of terminated employees and the user account access privileges for a sample of in-scope systems to determine that access was revoked for each in-scope system sampled.	No exceptions noted.
CC6.2.3	Users with access to in-scope systems are reviewed by management on an at least semi-annual basis to ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inspected the completed access review during the review period to determine that users with access to in-scope systems are reviewed by management on an at least semi-annual basis to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
	AWS and Rackspace are responsible for managing logical access to the underlying network, virtualization management, and storage devices for the encrypted backup storage and cloud hosting services where the Planview systems reside.		
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.			
CC6.3.1	Internal user access requests to the in-scope systems are documented and require the approval of IT Management.	Inspected the access approval documentation for a sample of users provided access during the review period to determine that internal user access requests to the in-scope systems were documented and approved by IT Management for each user sampled.	No exceptions noted.
CC6.3.2	Upon termination of an employee or a contractor, access to in-scope systems is revoked unless appropriate approval is obtained to extend access.	Upon termination of an employee or a contractor, access to in-scope systems is revoked unless appropriate approval is obtained to extend access.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.3	Administrative access privileges to the in-scope systems are restricted to user accounts for employees who require access and are authorized for such.	Inspected the administrative user listings for a sample of in-scope systems with the assistance of senior manager of hosting operations to determine that administrative access privileges to each in-scope system sampled were restricted to user accounts for employees who required access and were authorized for such.	No exceptions noted.
CC6.3.4	Users with access to in-scope systems are reviewed by management on an at least semi-annual basis to ensure that access to data is restricted and authorized. Accounts identified as inappropriate are investigated and resolved.	Inspected the completed access review during the review period to determine that users with access to in-scope systems are reviewed by management on an at least semi-annual basis to ensure that access to data was restricted and authorized and that accounts identified as inappropriate were investigated and resolved.	No exceptions noted.
	AWS and Rackspace are responsible for managing logical access to the underlying network, virtualization management, and storage devices for the encrypted backup storage and cloud hosting services where the Planview systems reside.		
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.			
	AWS, Rackspace and GoodData are responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.		
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.			
	AWS and Rackspace are responsible for managing logical access to the underlying network, virtualization management, and storage devices for the encrypted backup storage and cloud hosting services where the Planview systems reside.		
	AWS, Rackspace and GoodData are responsible for restricting physical access to data center facilities, backup data, and other system components such as virtual systems and servers.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Systems designed to manage and define network boundaries are in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that is not explicitly authorized by a rule.	Inspected the system configurations to determine that systems designed to manage and define network boundaries were in place to filter unauthorized inbound network traffic from the Internet and configured to deny any type of network connection that was not explicitly authorized by a rule.	No exceptions noted.
CC6.6.2	An encrypted VPN is required for remote access to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN authentication and encryption configurations to determine that an encrypted VPN was required for remote access to help ensure the security and integrity of the data passing over the public network.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.6.3	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS certificates to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.6.4	Penetration testing is performed on an annual basis by a third-party vendor. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected the penetration testing report and remediation plan to determine that penetration testing was performed during the review period by a third-party vendor and that identified critical and high severity security vulnerabilities were evaluated and addressed.	No exceptions noted.
CC6.6.5	Vulnerability scans are performed on an at least quarterly basis. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected the vulnerability scan schedule configuration, example scan report and remediation plan to determine that vulnerability scans were completed on an at least quarterly basis and identified critical and high severity security vulnerabilities were evaluated and addressed.	No exceptions noted.
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.			
CC6.7.1	An encrypted VPN is required for remote access to help ensure the security and integrity of the data passing over the public network.	Inspected the VPN authentication and encryption configurations to determine that an encrypted VPN was required for remote access to help ensure the security and integrity of the data passing over the public network.	No exceptions noted.
CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the TLS certificates to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.7.3	A device management tool is configured to manage and encrypt employee workstations.	Inspected the device management tool configurations to determine that a device management tool was configured to manage and encrypt employee workstations.	No exceptions noted.
CC6.7.4	Production customer data is encrypted at rest. Access to the cryptographic keys is restricted to authorized personnel.	Inspected the encryption configurations for a sample of in-scope servers to determine that production customer data was encrypted at rest for each server sampled and access to the cryptographic keys was restricted to authorized personnel.	The test of the control activity disclosed that production customer data was not encrypted at rest for one of 14 in-scope servers in Frankfurt.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.8.1	Antivirus software is utilized to protect registered Windows and Mac workstations and configured for real-time protection or scheduled scan.	Inspected the enterprise antivirus software configurations to determine that antivirus software was utilized to protect registered Windows and Mac workstations and configured for real-time protection.	No exceptions noted.
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.			
CC7.1.1	Penetration testing is performed on an annual basis by a third-party vendor. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of penetration testing completed by a third-party vendor to determine that identified critical and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
CC7.1.2	Vulnerability scans are performed on an at least quarterly basis. Identified critical and high severity security vulnerabilities are evaluated and addressed.	Inspected evidence of vulnerability scan completion and scan tool configurations to determine that vulnerability scans are completed on at least a quarterly basis and high severity security vulnerabilities are evaluated and addressed.	No exceptions noted.
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.			
CC7.2.1	Enterprise monitoring applications are configured to monitor the in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	Inspected evidence of enterprise monitoring application configurations and example alert to determine that enterprise monitoring applications are configured to monitor in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	No exceptions noted.
	AWS, Rackspace and GoodData are responsible for monitoring physical access to the data center facilities that house the production backup media, and other system components such as firewalls, routers, and servers.		
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.			
CC7.3.1	Documented incident response policy is communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	Observed the presence of the incident response policy on the company intranet to determine that a documented incident response policy was communicated to internal users via the company intranet.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the incident response policy to determine that a documented incident response policy was in place to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	No exceptions noted.
CC7.3.2	SecOps personnel utilize an automated ticketing system to document, evaluate, and track identified security events through resolution.	Inquired of the director of information security regarding incident response management to determine that a formal policy was in place for documenting, evaluating, and tracking identified security events through resolution.	No exceptions noted.
		Inspected the incident ticket for several examples of security events identified during the review period to determine that SecOps personnel utilized an automated ticketing system to document, evaluate, and track through to resolution, each security event sampled.	No exceptions noted.
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.			
CC7.4.1	Documented incident response policy is communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	Observed the presence of the incident response policy on the company intranet to determine that a documented incident response policy was communicated to internal users via the company intranet.	No exceptions noted.
		Inspected the incident response policy to determine that a documented incident response policy was in place to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	No exceptions noted.
CC7.4.2	SecOps personnel utilize an automated ticketing system to document, evaluate, and track identified security events through resolution.	Inquired of the director of information security regarding incident response management to determine that a formal policy was in place for documenting, evaluating, and tracking identified security events through resolution.	No exceptions noted.
		Inspected the incident ticket for several examples of security events identified during the review period to determine that SecOps personnel utilized an automated ticketing system to document, evaluate, and track through to resolution, each security event tested.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Documented incident response policy is communicated to internal users via company intranet to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	Observed the presence of the incident response policy on the company intranet to determine that a documented incident response policy was communicated to internal users via the company intranet.	No exceptions noted.
		Inspected the incident response policy to determine that a documented incident response policy was in place to guide users in identifying, reporting, and responding to system failures, incidents, and breaches.	No exceptions noted.
CC7.5.2	SecOps personnel utilize an automated ticketing system to document, evaluate, and track identified security events through resolution.	Inquired of the director of information security regarding incident response management to determine that a formal policy was in place for documenting, evaluating, and tracking identified security events through resolution.	No exceptions noted.
		Inspected the incident ticket for several examples of security events identified during the review period to determine that SecOps personnel utilized an automated ticketing system to document, evaluate, and track through to resolution, each security event sampled.	No exceptions noted.
CC7.5.3	SecOps and operations personnel complete incident postmortem reports that include the incident and impact analysis, resolutions, lessons learned, and action items.	Inquired of the director of information security regarding incident response management to determine that a formal policy was in place for documenting and producing to interested parties, a postmortem report for resolved incidents that included the incident and impact analysis, resolutions, lessons learned, and action items.	No exceptions noted.
		Inspected the postmortem report for several examples of security events resolved during the review period to determine that SecOps and operations personnel completed an incident postmortem report that included the incident and impact analysis, resolution, lessons learned, and action items for each security event tested.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC8.1.1	Change management policies and processes for new releases to production environment are in place.	Inspected the change management policies and processes to determine that change management policies and processes for new releases to production environment were in place.	No exceptions noted.
CC8.1.2	Changes are authorized, tested, and approved prior to deployment.	Inspected the change documentation for a sample of changes implemented during the review period to determine that changes were authorized, tested, and approved prior to deployment for each change sampled.	No exceptions noted.
CC8.1.3	The production environment is logically segregated from development environment.	Inspected the production and development environment server listings to determine that the production environment was logically segregated from development environment.	No exceptions noted.
CC8.1.4	The ability to implement application changes via the automated deployment tool is restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with write access to application source code and the listing of users with the ability to implement application changes via the automated deployment tool to determine that the ability to implement changes via the automated deployment tool was restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.5	Version control software is utilized to restrict access to application source code and provide rollback capabilities.	Inspected the version control software configurations to determine that version control software was utilized to restrict access to application source code and provide rollback capabilities.	No exceptions noted.
CC8.1.6	Write access to the version control software is restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with write access to application source code to determine that write access to the version control software was restricted to user accounts accessible by authorized personnel.	The test of the control activity disclosed that one user had write access to application source code in excess of their job responsibilities. Additional testing disclosed that the aforementioned user did not make any application source code changes during the review period.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	Management perform a risk assessment on an annual basis that includes an evaluation of risk mitigation control activities for risks arising from potential business disruptions.	Inspected the risk register documentation to determine that management performed a risk assessment on an annual basis that included an evaluation of risk mitigation control activities for risks arising from potential business disruptions.	No exceptions noted.
CC9.1.2	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved on an annual basis	Inspected the business continuity plan including evidence of plan approval to determine that business continuity and disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected evidence of business continuity plan review and approval by the Security Steering Committee to determine that the plans were reviewed, updated, and approved during the review period.	No exceptions noted.
CC9.1.3	Business continuity and disaster recovery plans are tested on at least an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the results of the business continuity plan to determine that the business continuity plan was tested during the review period.	The test of the control activity disclosed that the business continuity plan was tested in December 2018, prior to the review period.
		Inspected the results of the disaster recovery plan to determine that the disaster recovery plan was tested during the review period.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Management reviews audit reports from third-party service providers on an annual basis and evaluates subservice organization controls and user-entity controls considerations to help ensure compliance with security and availability commitments and system requirements.	Inspected evidence of management review of audit reports for a sample of third-party service providers to determine that management review the audit reports of each third-party service provider sampled.	No exceptions noted.

[Intentionally Blank]

ADDITIONAL CRITERIA FOR AVAILABILITY

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	Enterprise monitoring applications are configured to monitor the in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	Inspected evidence of enterprise monitoring application configurations and example alert to determine that enterprise monitoring applications are configured to monitor in-scope systems for performance and availability and alert operations personnel when predefined thresholds have been met.	No exceptions noted.
A1.1.2	The CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	Inspected evidence of monthly system performance meetings and noted that the CIO meets with stakeholders monthly to review overall system performance and its impact on availability and security.	No exceptions noted.
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2.1	An automated backup system is configured to perform scheduled backups of production data at least daily and notify operations personnel regarding the failure of backup jobs.	Inspected the backup configurations for a sample of servers and example backup failure alert to determine that an automated backup system was configured to perform scheduled backups of production data at least daily for each server sampled and notify operations personnel regarding the failure of backup jobs.	No exceptions noted.
A1.2.2	Backup data is configured to be retained for 30 days.	Inspected the backup retention configurations for a sample of servers to determine that backup data was configured to be retained for 30 days for each server sampled.	No exceptions noted.
A1.2.3	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved on an annual basis.	Inspected the business continuity plan including evidence of plan approval to determine that business continuity and disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of business continuity plan review and approval by the Security Steering Committee to determine that the plans were reviewed, updated, and approved during the review period.	No exceptions noted.
A1.2.4	Business continuity and disaster recovery plans are tested on at least an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the results of the business continuity plan test to determine that the business continuity plan was tested during the review period.	Refer to the test results for control activity CC9.1.3.
		Inspected the results of the disaster recovery plan test to determine that the disaster recovery plan was tested during the review period.	No exceptions noted.
	AWS, Rackspace and GoodData are responsible for ensuring the data center facilities are equipped with environmental security safeguards.		
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Business continuity and disaster recovery plans are in place to guide personnel in procedures to protect against disruptions caused by an unexpected event. The plans are reviewed, updated, and approved on an annual basis	Inspected the business continuity plan including evidence of plan approval to determine that business continuity and disaster recovery plans were in place to guide personnel in procedures to protect against disruptions caused by an unexpected event.	No exceptions noted.
		Inspected evidence of business continuity plan review and approval by the Security Steering Committee to determine that the plans were reviewed, updated, and approved during the review period.	No exceptions noted.
A1.3.2	Business continuity and disaster recovery plans are tested on at least an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the results of the business continuity plan test to determine that the business continuity plan was tested during the review period.	Refer to the test results for control activity CC9.1.3.
		Inspected the results of the disaster recovery plan test to determine that the disaster recovery plan was tested during the review period.	No exceptions noted.

Section 5

Other Information Provided by Planview

MANAGEMENT'S RESPONSE TO TESTING EXCEPTIONS

Security

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.1.2 CC1.4.3	Educational and background checks are performed for employees as a component of the hiring process.	Inspected evidence of educational and background checks for a sample of employees hired during the review period to determine that educational and criminal background checks were performed for each employee sampled.	The test of the control activity disclosed that educational and criminal background checks were not evidenced for one of 25 employees sampled.
Management's Response:	Planview is committed to ensuring that background checks are performed before an employee is made an offer of employment. The employee referenced in the finding listed underwent a background check prior to employment. Evidence of the background check was provided outside the review period due to communication delays with the vendor who conducts the checks and provides reports of the results.		
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.			
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC1.3.2 CC1.4.2 CC1.5.1 CC2.2.3	Job descriptions are defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system.	Inspected evidence of job descriptions for a sample of employment positions to determine that job descriptions were defined, describing the skills, responsibilities, and knowledge levels required for employees with access to or supporting the system for each employment position sampled.	The test of the control activity disclosed that defined job descriptions were not evidenced for four of 25 job descriptions sampled.
Management's Response:	Planview is committed to ensuring that personnel who have access to production systems are fully aware of their responsibilities. The four job descriptions not evidenced during the review period are unavailable due to record synchronization issues related to merger/acquisition and migration of workforces into the existing Planview workforce.		

[Intentionally Blank]

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
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.			
CC6.7.4	Production customer data is encrypted at rest. Access to the cryptographic keys is restricted to authorized personnel.	Inspected the encryption configurations for a sample of in-scope servers to determine that production customer data was encrypted at rest for each server sampled and access to the cryptographic keys was restricted to authorized personnel.	The test of the control activity disclosed that production customer data was not encrypted at rest for one of 14 in-scope servers in Frankfurt.
Management's Response:	Planview is committed to ensuring that customer data is encrypted at rest. The unencrypted database in Frankfurt was the result of an oversight in the instance implementation process; the database encryption was applied in October 2019. Spigit team members have begun to develop monitoring and alerting rules to capture the encryption status to ensure anomalies are reported in a timely manner.		
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.			
CC8.1.6	Write access to the version control software is restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with write access to application source code and the listing of users with the ability to implement application changes via the automated deployment tool to determine that write access to the version control software was restricted to user accounts accessible by authorized personnel.	The test of the control activity disclosed that one user had write access to application source code in excess of their job responsibilities. Additional testing disclosed that the aforementioned user did not make any application source code changes during the review period.
Management's Response:	Planview is committed to ensuring that separation of duties is enabled to the extent possible and to ensure that monitoring and alerting are in place to capture anomalies in related processes.		

Security and Availability

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
CC9.1.3 A1.2.5 A1.3.2	Business continuity and disaster recovery plans are tested on at least an annual basis to help ensure the production environment can be recovered in the event of a disaster.	Inspected the results of the business continuity plan to determine that the business continuity plan was tested during the review period.	The test of the control activity disclosed that the business continuity plan was tested in December 2018, prior to the review period.
Management's Response:	Planview is committed to ensuring that business continuity is tested annually, and the established cadence for this testing ensures that it occurs in or around the last month of the year. Because the audit period for the Spigit solution started in March and ended in October, the standard test window for business continuity falls outside the audit period.		