Report on Smartsheet Inc.'s Cloud-Based Platform Relevant to Security, Availability, Processing Integrity, and Confidentiality Throughout the Period September 1, 2021 to August 31, 2022

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: Smartsheet Inc. ("Smartsheet")

Scope

We have examined Smartsheet's accompanying assertion titled "Assertion of Smartsheet Inc. Management" (assertion) that the controls within Smartsheet's Cloud-Based Platform (system) were effective throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity and confidentiality (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Service Organization's Responsibilities

Smartsheet 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 Smartsheet's service commitments and system requirements were achieved. Smartsheet has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Smartsheet is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Smartsheet's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Smartsheet's service commitments and system requirements based on the applicable trust services criteria.

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

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the examination engagement.

Inherent Limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within Smartsheet's Cloud-Based Platform were effective throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Coalfire Controls LLC

Westminster, Colorado
November 15, 2022

Section 2

Assertion of Smartsheet Inc. Management

Assertion of Smartsheet Inc. ("Smartsheet") Management

We are responsible for designing, implementing, operating and maintaining effective controls within Smartsheet's Cloud-Based Platform (system) throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that Smartsheet's service commitments and system requirements relevant to security, availability, processing integrity, and confidentiality were achieved. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period September 1, 2021 to August 31, 2022, to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, processing integrity, and confidentiality (applicable trust services criteria) set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria). Smartsheet's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in attachment B.

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

We assert that the controls within the system were effective throughout the period September 1, 2021 to August 31, 2022 to provide reasonable assurance that Smartsheet's service commitments and system requirements were achieved based on the applicable trust services criteria.

Smartsheet Inc.

Chris Peake
Chief Information Security Officer

Attachment A

Smartsheet Inc.’s Description of the Boundaries of Its Cloud-Based Platform

Type of Services Provided

Smartsheet Inc. (“Smartsheet” or “the Company”) is a software-as-a-service (SaaS) company that was formed in 2006 and is headquartered in Bellevue, WA. Smartsheet offers its Cloud-Based Platform for collaborative work management to help enable teams and organizations to plan, capture, track, automate, and report on work at scale in an effort to improve processes and business outcomes. Smartsheet’s Cloud-Based Platform is used by businesses and users in countries throughout the world. Customers range from small and medium-sized businesses to Fortune 500 companies and academic institutions, as well as local and federal government agencies.

Smartsheet’s Cloud-Based Platform provides a number of solutions to help eliminate obstacles to capturing information, including a spreadsheet interface and customizable forms. The reporting and automation capabilities have been designed to help reduce time spent on administration and repetitive work and allow teams to apply business logic to automate repetitive actions using a list of conditions. Business users can configure and modify the platform to customize workflows to suit their needs. The user interface and functionality help users utilize the platform without changing the behaviors developed using lightweight productivity tools. Customers access the platform online via a website, mobile applications for Android and iOS, or web service integrations.

Smartsheet’s Cloud-Based Platform offers extended capabilities through its premium product offerings to its customers, represented as add-ons to the core Smartsheet functionality. Smartsheet’s Cloud-Based Platform represents the collective of these products and services:

Product Name	Description
Smartsheet	Smartsheet enables teams to plan, capture, manage, automate, and report on work and get up to speed fast. Users can edit and easily share work in grid, card, Gantt, or calendar views. Smartsheet also enables users to capture data with forms and to automate workflows and repetitive tasks. Users can create and share dashboards and reports in a short time and have access to integrations with various chat tools.
Brandfolder	Using unique visual tools, Brandfolder quickly and easily organizes, curates, and distributes brand assets, making it easy to increase brand consistency and engagement. The configurable platform also allows administrators to customize the experience for any need, beginning with highly curated “press kits” to archive-scale storage for a brand’s content.
Resource Management by Smartsheet	Resource Management by Smartsheet (formerly 10,000ft) is a resource management solution for building teams, keeping project schedules and budgets on track, and forecasting business needs.
Accelerators	Accelerators help business owners programmatically solve common challenges with pre-configured solutions.
Control Center	Control Center is a project and portfolio management solution that delivers consistent, visible projects and processes at scale with best practices for work execution, reporting, and risk management built in.
Dynamic View	Dynamic View enables business owners to manage multi-step processes by sharing only what is needed to the right people at the right time for viewing or editing.
DataMesh	The DataMesh app allows users to map large volumes of data across sheets.

Product Name	Description
Data Shuttle	Data Shuttle by Smartsheet allows users to upload or offload data between Smartsheet and their Enterprise Resource Planning (ERP) and Customer Relationship Management (CRM) tools, and databases. This enables users to automatically centralize their data into one source.
Pivot App	Pivot App enables users to automatically categorize and summarize data stored in Smartsheet.
Calendar App	Calendar App allows users to build interactive and shareable calendars with custom details.
Bridge by Smartsheet	Bridge by Smartsheet is a no-code, cross-platform process automation engine that enables users to connect data across systems and automates routine tasks.
Connectors	Connectors for Salesforce, Jira, Microsoft Dynamics 365, and more provide real-time visibility into critical business systems.
WorkApps	WorkApps is a no-code platform for building intuitive web and mobile apps.
Event Reporting	Event Reporting helps to ensure organizational compliance by providing visualization of granular details of who is doing what in Smartsheet and when. Users can identify abnormal behavior and affirm that data is being used within established guardrails.
Customer Managed Encryption Keys (CMEK)	CMEK enables users to control access to data at rest in their sheets. With CMEK, users can monitor, grant, and revoke access to their data using their own key, stored outside of Smartsheet.
Governance Policies	The Data Retention Policy allows customers to set their own criteria on when, and if, they want to delete data that is no longer relevant.

The Components of the System Used to Provide the Services

The boundaries of Smartsheet's Cloud-Based Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Smartsheet's Cloud-Based Platform.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes third-party cloud services providers to provide the resources to host Smartsheet's Cloud-Based Platform. The Company leverages the experience and resources of the third-party cloud services providers to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring Smartsheet's Cloud-Based Platform architecture within the third-party cloud services providers to ensure the availability, security, and resiliency requirements are met.

The in-scope hosted infrastructure also consists of multiple supporting tools to address the following business functions:

- Customer data and metadata storage
- Hosting Smartsheet's Cloud-Based Platform
- Network segmentation and security

Software

Software consists of the programs and software that support Smartsheet's Cloud-Based Platform (operating systems [OSs], middleware, and utilities). Smartsheet uses various third-party applications to perform the following business functions:

- Application monitoring
- Backup and replication
- Security information and event management (SIEM) and logging system
- Infrastructure monitoring
- Deployment and Configuration management
- Vulnerability management
- Endpoint antivirus

People

Smartsheet maintains multiple discipline-aligned teams to promote secure development practices while minimizing total time to market for approved features. Smartsheet Quality Assurance (QA) personnel perform both automated and manual testing, as applicable, of all product releases. The Infrastructure and Operations teams are responsible for product delivery and providing design input as needed. These roles ensure adequate capacity and approval, as well as implementation of scaling plans. The Security team is involved in all stages of application development, testing, and delivery to act as the primary stewards of customer trust and data integrity.

The Company develops, manages, and secures Smartsheet's Cloud-Based Platform via separate departments. The responsibilities of these departments are defined in the following table:

People	
Group/Role Name	**Function**
Executive Management	Responsible for overseeing company-wide activities, establishing, and accomplishing goals, and managing objectives.
Engineering	Responsible for the development, testing, deployment, and maintenance of new code and infrastructure for Smartsheet's Cloud Based Platform.
Security	Responsible for managing access controls and the security of the production environment.
Governance, Risk, and Compliance	Responsible for policy development, security governance, security awareness training, and support of security initiatives in all divisions of the organization.
Legal	Responsible for handling contractual agreements, litigation incidents, and the management and maintenance of Smartsheet's privacy program.

People	
Group/Role Name	**Function**
Privacy	Responsible for the management of the internal privacy program at Smartsheet.
Product Management	Responsible for overseeing the product life cycle, including adding new product functionality.
People & Culture (P&C)	Responsible for onboarding new personnel, defining the roles and positions of new hires, performing background checks, and facilitating the employee termination process.
Information Technology	Responsible for implementing and maintaining desktop support and IT-related functions.
Workplace Services	Responsible for office and facility operations, managed through the lens of providing the best possible employee experience.

The following organization chart reflects the Company's internal structure related to the groups discussed above:

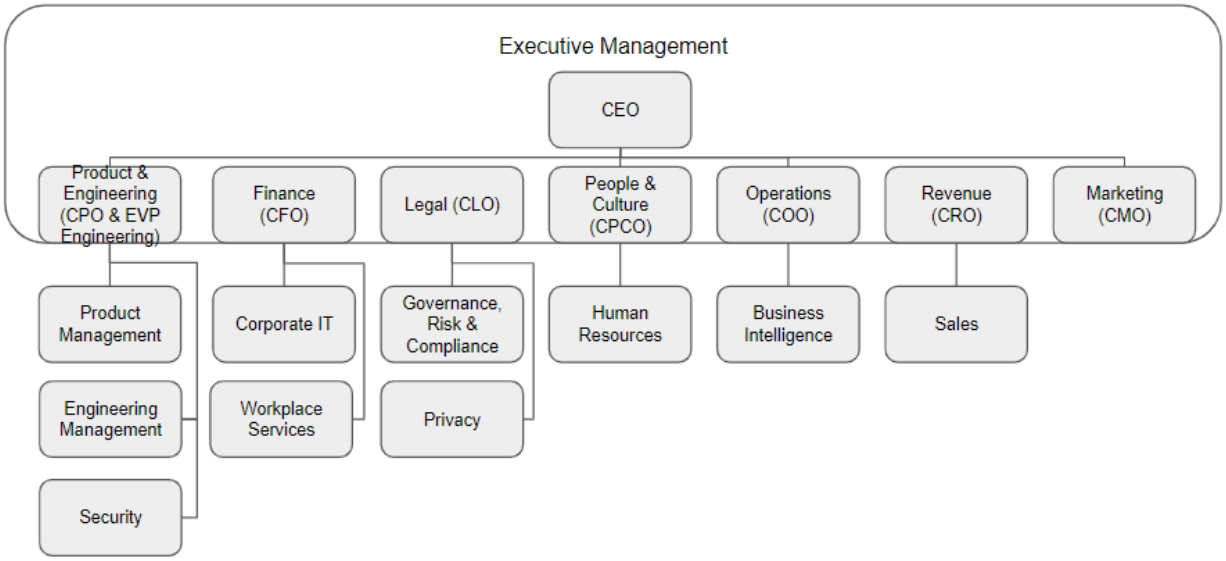

Figure 1: Smartsheet Organization Chart

Procedures

Procedures include the automated and manual procedures involved in the operation of Smartsheet's Cloud-Based Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to product and engineering, technical operations, security, information technology (IT), and People & Culture (P&C). These procedures are drafted in alignment with the overall information security policies and are updated and approved as necessary for changes in the business, but no less than annually.

The following table details the procedures as they relate to the operation of Smartsheet's Cloud-Based Platform:

Procedures	
Procedure	**Description**
Logical Access	How the Company restricts logical access, provides and removes that access, and prevents unauthorized access.
System Operations	How the Company manages the operation of the system and detects and mitigates processing deviations, including logical security deviations.
Change Management	How the Company identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
Risk Mitigation	How the Company identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.
Data Retention	How the Company consistently protects data and information assets throughout their life cycle and in accordance with current laws and regulations.
Incident Response	How the Company identifies and responds to suspected or known security incidents and mobilizes the Incident Response Team (IRT) to mitigate the harmful effects of security incidents and to document the incidents and outcomes.

Data

Smartsheet processes customer data in one of two categorizations. Customer relationship data is data provided by customers to facilitate the business relationship (e.g., billing addresses, email addresses, application preferences). Customer relationship data is available to personnel at Smartsheet based on need to know and is governed by corporate IT controls. Protected customer data is any data that is uploaded or submitted to Smartsheet's Cloud-Based Platform by the customer or collected by the customer through use of forms or similar features. Ownership of protected customer data is dictated directly by the customer and any designated system administrators for that customer. Any access to protected customer data by Smartsheet personnel is governed by one of two mechanisms:

- The primary means of access is for the customer to explicitly share protected customer data with Smartsheet personnel as they would any other collaborator within Smartsheet's Cloud-Based Platform. This interaction is then governed by the same controls that would apply to any Smartsheet customer. There is no additional access available to Smartsheet personnel by nature of that sharing action.
- The secondary means of access is limited to Smartsheet core team operations specialists who have been specifically trained and approved. For example, direct access may be granted in order to investigate potential abuse of Smartsheet's Cloud-Based Platform or to respond to lawful requests for protected customer data, such as a subpoena. This secondary means is outlined to customers in the agreements that govern their use.

The following table details the types of data contained in the production application for Smartsheet's Cloud-Based Platform:

Data	
Production Application	**Description**
Business Intelligence and Telemetry Data	The Company keeps track of user activity in relation to the types of services customers and their users use, the configuration of their computers, and performance metrics related to their use of the services.
Protected Customer Data	The Company logs information about customers and their users, including Internet Protocol (IP) address. Log files are immutable records of computer events about an OS, application, or user activity, which form an audit trail. These records may be used to assist in detecting security violations, performance problems, and flaws in applications.

Subservice Organizations

The Company uses subservice organizations for data center colocation services. The Company's controls related to Smartsheet's Cloud-Based Platform cover only a portion of the overall internal control for each user entity of Smartsheet's Cloud-Based Platform. The description does not extend to the colocation services for IT infrastructure provided by the subservice organizations.

Although the subservice organizations have been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organizations. Controls are expected to be in place at the subservice organizations related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. The subservice organization's physical security controls should mitigate the risk of unauthorized access to the hosting facilities. The subservice organizations' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

The Company management receives and reviews the subservice organizations' SOC 2 reports annually. In addition, through its operational activities, Company management monitors the services performed by the subservice organizations to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organizations to monitor compliance with the service agreements, stay informed of changes planned at the hosting facilities, and relay any issues or concerns to management of the subservice organizations.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Smartsheet's Cloud-Based Platform. Commitments are communicated in Smartsheet's Service Agreements.

System requirements are specifications regarding how Smartsheet's Cloud-Based Platform should function to meet the Company's principal commitments to user entities. System requirements are specified in the Company's policies and procedures.

The Company's principal service commitments and system requirements related to Smartsheet's Cloud-Based Platform include the following:

Trust Services Category	Service Commitments	System Requirements
Security	• Smartsheet shall maintain a comprehensive written information security program, including policies, standards, procedures, and related documents that establish criteria, means, methods, and measures governing the processing and security of customer content. • Smartsheet will implement and maintain information security policies and safeguards including physical, organizational, and technical measures designed to preserve the security, integrity, and confidentiality of customer data and protect against information security threats. • Smartsheet shall protect customer data from known or reasonably anticipated threats or hazards to its security, integrity, accidental loss, alteration, disclosure, and other unlawful forms of processing.	• Employee provisioning and deprovisioning standards • Logical access controls, such as the use of user IDs and passwords to access systems • Access reviews • Incident handling standards • Vendor management • System monitoring • Risk assessment standards • Change management controls • Monitoring controls
Availability	• Smartsheet will ensure a monthly system uptime of at least 99.9%. • Smartsheet will maintain a disaster recovery program designed to recover the service's availability following a disaster.	• Backup and recovery standards
Processing Integrity	• Smartsheet will implement and maintain information security policies and safeguards including physical, organizational, and technical measures designed to preserve the security, integrity, and confidentiality of customer data and protect against information security threats. • Smartsheet shall protect customer data from known or reasonably anticipated threats or hazards to its security, integrity, accidental loss, alteration, disclosure, and other unlawful forms of processing.	• Employee provisioning and deprovisioning standards • Logical access controls, such as the use of user IDs and passwords to access systems • Access reviews • Maintaining internal privacy and data handling policies and procedures • Ensuring applicable personnel are appropriately trained

Trust Services Category	Service Commitments	System Requirements
Confidentiality	• Smartsheet will not disclose confidential customer data for any purpose except for providing the service. • Smartsheet will not disclose, give access to, or distribute any customer data to third parties except as authorized in providing the services or in a written agreement signed by the customer. • Smartsheet will take reasonable security precautions, at least as protective as their own precautions, to safeguard customer data. • Smartsheet will promptly notify customers, in writing, upon discovery of any unauthorized disclosure or use of customer data. • Smartsheet will return, destroy, or delete all customer data upon customer's written request.	• Data classification • Data handling standards