



SLACK TECHNOLOGIES, LLC.

INDEPENDENT SERVICE AUDITOR'S SOC 3 REPORT
FOR THE GOVSLACK TEAM COLLABORATION PLATFORM
FOR THE PERIOD OF JULY 1, 2022, TO JANUARY 31, 2023

Attestation and Compliance Services



Proprietary & Confidential

Unauthorized use, reproduction, or distribution of this report, in whole or in part, is strictly prohibited.

INDEPENDENT SERVICE AUDITOR'S REPORT

To Slack Technologies, LLC.:

Scope

We have examined Slack Technologies, LLC.'s ("Slack Technologies") accompanying assertion titled "Assertion of Slack Technologies, LLC. Service Organization Management" ("assertion") that the controls within Slack Technologies' GovSlack Team Collaboration Platform system ("system") were effective throughout the period July 1, 2022, to January 31, 2023, to provide reasonable assurance that Slack Technologies' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)*.

Slack Technologies uses various subservice organizations for cloud hosting, board of directors' oversight, HR functions, vendor management, and endpoint management services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Slack Technologies, to achieve Slack Technologies' service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system 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 description of the boundaries of the system indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Slack Technologies, to achieve Slack Technologies' service commitments and system requirements based on the applicable trust services criteria. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and systems 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 Slack Technologies' service commitments and system requirements based on the applicable trust services criteria; and
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Slack Technologies' service commitments and system requirements based on the applicable trust services criteria.

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

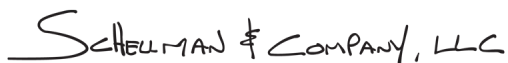
Inherent limitations

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that Slack Technologies' 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 Slack Technologies' GovSlack Team Collaboration Platform system were effective throughout the period July 1, 2022, to January 31, 2023, to provide reasonable assurance that Slack Technologies' service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

SCHHELLMAN & COMPANY, LLC

Tampa, Florida
March 15, 2023

ASSERTION OF SLACK TECHNOLOGIES SERVICE ORGANIZATION MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Slack Technologies, LLC.'s ("Slack Technologies") GovSlack Team Collaboration Platform system ("system") throughout the period July 1, 2022, to January 31, 2023, to provide reasonable assurance that Slack Technologies' service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented below 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 July 1, 2022, to January 31, 2023, to provide reasonable assurance that Slack Technologies' service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (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)*. Slack Technologies' objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and systems requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented below.

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 July 1, 2022, to January 31, 2023, to provide reasonable assurance that Slack Technologies' service commitments and systems requirements were achieved based on the applicable trust services criteria.

DESCRIPTION OF THE BOUNDARIES OF THE GOVSLACK TEAM COLLABORATION PLATFORM SYSTEM

Company Background

Since 2014, Slack Technologies, LLC (“Slack Technologies”, “Slack”, or the “Company”) has provided the Team Collaboration Platform called “Slack” (the “System”) to businesses and organizations (“user entities”), designed to ensure the right people are always in the loop and key information is always at their fingertips. Beginning in 2022, a new dedicated instance of Slack, known as GovSlack, was released. GovSlack was designed to support key government regulations for processing and storing sensitive data while still offering the same flexibility offered by Slack. Slack Technologies was acquired by Salesforce, Inc. (“Salesforce”) on July 21, 2021. As a result of this acquisition, the design and operation of several entity level control activities have been transferred from Slack Technologies to Salesforce. Refer to the “Complementary Subservice Organization Controls” section for the complete listing of control activities that Salesforce is responsible for.

Collectively, the Slack GovSlack Team Collaboration Platform (“GovSlack”) consists of:

- GovSlack Native Client Applications
- GovSlack Web Applications and Services
- GovSlack Application Programming Interfaces (“APIs”)

With GovSlack, users join a secure instance called a “Workspace” (“Slack Workspace”) where members can message each other in real time individually or in groups across multiple device types. Discussions can be organized into different topics (called “channels”) or different groups of Workspace members, as desired. Slack Workspaces can connect to one another, and all members within an organization share a directory. As a collaboration hub, GovSlack allows other services to connect into the different discussions, providing updates and notifications directly into GovSlack. GovSlack provides a valuable repository of information by capturing all communication and content in one archive that is searchable.

GovSlack integrates with a large number of third-party services and supports community-built integrations. GovSlack provides mobile apps for iOS and Android in addition to their web browser client and electron desktop clients for macOS, Windows, and Linux (beta). GovSlack has been used for organizational communication, as well as a community platform.

GovSlack offers a set of development tools to help customers integrate third-party services and build custom workflow automations. Using GovSlack APIs, developers can build custom applications with tools like the d software development kit (SDK). Users can create workflows using Workflow Builder, a no-code automation tool built natively into GovSlack.

Additional detail is posted on the Company’s website and made available to internal and external users.

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.

Principal Service Commitments and System Requirements

Principal Service Commitments

Slack makes the following security, availability, and confidentiality commitments to their customers: These commitments are made available to the public on Slack's website (<https://slack.com/security-practices>).

- Slack will make the services available 99.99% of the time, except for maintenance or as otherwise provided in service level agreement (SLA) described in the service contract;
- Production cloud infrastructure hosted within multiple geographically diverse availability zones/regions;
- Encrypt data in transmission using transport layer security (TLS) or other technologies over public networks;
- Maintain commercially reasonable administrative, technical, and organizational to protect the security of customer data against anticipated threats or hazards;
- Confidential data stored within the production services utilize advanced encryption standard (AES) encryption;
- Confidential data stored within the production services is retained per customer defined retention policies; and
- Disaster recovery plans are in place and tested at least once per year.

System Requirements

Slack has put into place a set of policies and procedures, inclusive of technology-based controls and automation, to help ensure that security, availability, and confidentiality commitments are met.

Slack's commitments to security, availability, and confidentiality are described in the standard service agreement contracts for contracted customers. Customers are required to sign the Terms of Service agreement prior to receiving Slack's services. These agreements describe the technical and organizational controls that Slack is responsible for maintaining for their customers.

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.

Infrastructure

The System production environment is hosted by infrastructure subprocessors. The Company maintains the list of current subprocessors here: <https://slack.com/slack-subprocessors>, which included Amazon Web Services (AWS) among others during the period covered by this report. Development occurs on systems in environments that are separate from the production environment.

Customer data is processed by and stored in hosted infrastructure compute services (such as Amazon Elastic Compute Cloud (EC2) instances and hosted infrastructure storage services (such as Amazon Simple Storage Service (S3)). AWS S3 is also utilized to store backup copies of customer data. Amazon Simple E-mail Service (SES) is also utilized to receive e-mail-based communication with users.

Software

The System is implemented using Linux, Apache, Hypertext Processor (PHP), and MySQL technologies with well-understood performance, scalability, and security properties. The System's real-time service is implemented in Java using the WebSocket protocol.

People

The Company's control environment is implemented, maintained, and supported by Infrastructure Engineering, Security, Customer Experience, People Operations (People Ops), Business Technology (BizTech), Quality Assurance (QA), Legal, Product Development, and Executive Management. The Company's personnel are recruited and managed according to policies and procedures which are described in the *Summary of Control Activities* section below.

Processes

Formal policies and procedures codify the principles and requirements ensuring the security, availability, and confidentiality of the System. Personnel are required to adhere to the Company's policies and procedures, which are located on the Company's intranet and can be accessed by any Company personnel. These processes are detailed further in the *Summary of Control Activities* section below.

Data

The following table describes the information used and supported by the system.

Data Used and Supported by the System		
Data Description	Data Reporting	Classification
Customer data	Data available to customers in their designated Workspace via the desktop, web, or mobile applications.	Confidential and private to the customer

The System stores and processes information provided by user entities without inspection; such information is maintained as confidential and private to that user entity. This confidential and private information is available only to members of the user entity's GovSlack Workspace. Each user entity has designated administrators who authorize member access to information stored in their GovSlack Workspace.

As described below in the "Summary of Control Activities" section, access to customer data by Company personnel is restricted to authorized personnel. All other access to customer data by Company personnel requires management authorization or explicit approval from the user entity.

Subservice Organizations (Subprocessors)

The cloud hosting services provided by AWS; the service management services provided by ZenDesk; and the board of directors' oversight, HR functions, vendor management, and endpoint management services provided by Salesforce were not included within the scope of this examination. See the Complementary Subservice Organization Controls section below for more details.

Complementary Subservice Organization Controls (CSOCs)

The Company utilizes the following three (3) service organizations ("subservice organizations") to implement portions of the System: 1) Salesforce 2) AWS 3) Zendesk, Inc. (Zendesk). The AWS and Zendesk instances used to support GovSlack are separate from those used to support Slack Team Collaboration Platform.

Salesforce

The Company utilizes Salesforce for entity level control activities such as board of director's oversight, HR functions, vendor management, and endpoint management. Salesforce is responsible for maintaining an effective control environment which oversees various Slack processes.

Salesforce is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)*. This description includes only the controls of the System and does not include any of the controls expected to be implemented at Salesforce.

It is expected that Salesforce has implemented the following types of controls to support achievement of the associated criteria:

Controls Expected to be Implemented at Salesforce	
Applicable Trust Services Criteria	CSOCs
CC1.1, CC1.4	Salesforce is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; evaluating the competency of existing personnel; the employee handbook, and the code of conduct; defining job descriptions; and other HR functions that may relate to the stated criterion.
CC1.2	Salesforce is responsible for implementing controls that ensures the board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	Salesforce is responsible for implementing controls for defining job descriptions; communicating the defined lines of reporting to personnel; and other HR functions that establish authorities and responsibilities of personnel.
CC1.5	Salesforce is responsible for implementing controls for defining job descriptions; the employee sanction process; communication of performance metrics to the board of directors; and other corporate entity functions that may relate to the stated criterion.
CC2.1	Salesforce is responsible for implementing controls for providing security awareness training to employees and contractors and ensuring personnel certify acceptance of responsibilities upon completion of training.
CC2.2	Salesforce is responsible for implementing controls for new employee hiring policies and procedures; employment candidate screening and onboarding procedures; defining job descriptions; and other HR functions that may relate to the stated criterion.
CC2.3, C1.1	Salesforce is responsible for implementing controls communicating its security, privacy, and architecture documentation to Customers via the Trust website, which includes commitments to security, availability, and confidentiality.
CC3.1, CC3.4, CC4.1 CC9.2	Salesforce is responsible for implementing controls to evaluate vendor risk and other functions that may relate to the stated criterion.
CC3.4, CC9.2	Salesforce is responsible for implementing controls to evaluate data center hosting providers and sub-processers.
CC6.8	Salesforce is responsible for implementing controls for employee workstation security configurations which includes workstation antivirus, workstation encryption, workstation security updates, and workstation idle time logout configurations.
C1.1	Salesforce is responsible for implementing controls to require third parties with access to confidential customer data to sign an agreement with confidentiality provisions.

AWS

The Company utilizes services from AWS, such as EC2 for infrastructure hosting and S3 for data storage and AWS SES to send and receive e-mail-based communication with users. AWS is responsible for operating, managing, and controlling the components from the host operating system and virtualization layer and storage, down to the physical security and environmental controls over the facilities in which the services operate. AWS is examined annually in accordance with the *AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®)*. This description

includes only the controls of the System and does not include any of the controls expected to be implemented at AWS.

It is expected that AWS has implemented the following types of controls to support achievement of the associated criteria:

Controls Expected to be Implemented at AWS	
Applicable Trust Services Criteria	CSOCs
CC3.2, CC3.3	Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.
CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.
CC6.1	Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.
	The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
	Security measures are implemented to prevent unauthorized disclosure, usage, and/or access to confidential information.
CC6.2	Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
CC6.3	Logical access to the software and physical access to the software hosting datacenter facilities are provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
CC6.4, CC6.5	Physical access to the datacenter facilities is restricted to authorized personnel.
CC6.6	Logical security measures have been implemented to protect and detect external threats.
CC6.7	Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting users with the ability to do so.
CC6.8	Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
CC7.2	Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
CC7.3, 7.4, 7.5	Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
CC8.1	Software development lifecycle (SDLC) has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.
	Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.
	Procedures are established and implemented to ensure changes to systems are authorized, designed, developed, configured, documented, tested, and approved prior to production deployment.

Controls Expected to be Implemented at AWS	
Applicable Trust Services Criteria	CSOCs
CC8.1	Procedures are implemented to ensure confidential information is protected during systems change management processes.
CC9.2	Confidential information is only obtained in accordance with the defined commitments or agreements.
A1.1	Monitoring tools are implemented to monitor and manage the systems' capacity and availability.
A1.2	Environmental protections, data backup processes, recovery infrastructure, and monitoring and alarming mechanisms have been implemented to adequately address availability requirements.
A1.3	Business continuity/disaster recovery procedures are tested periodically.

ZenDesk

The Company utilizes Zendesk for receiving, managing, and resolving requests for assistance from its users. Zendesk is responsible for collecting and storing customer-submitted requests and providing help desk functionality for the Company's Customer Experience Department. Zendesk is examined annually in accordance with the AICPA Guide, Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy (SOC 2®). This description includes only the controls of the System and does not include any of the controls expected to be implemented at Zendesk.

It is expected that Zendesk has implemented the following types of controls to support achievement of the associated criteria:

Controls Expected to be Implemented at Zendesk	
Applicable Trust Services Criteria	CSOCs
CC3.2, CC3.3	Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality threats and/or risks.
CC4.1, CC4.2	Procedures are established and implemented to evaluate the designs and operating effectiveness of controls as they relate to security, availability, and/or confidentiality commitments, as well as to identify and track to resolution the corrective actions for control deficiencies.
CC6.1	Logical security has been implemented to authenticate authorized users, restrict access, prevent, and detect unauthorized access.
	The systems are configured to identify and authenticate internal and external users with appropriate valid credentials.
CC6.2	Procedures are implemented to provision and de-provision user access to systems and applications based on appropriate authorization.
CC6.3	Logical access to the software and physical access to the software hosting datacenter facilities are provisioned to authorized personnel and revoked upon termination or when access is no longer needed.
CC6.6	Logical security measures have been implemented to protect and detect external threats.
CC6.7	Logical security measures have been implemented to secure the transmission, movement, and removal of information, as well as restricting users with the ability to do so.

Controls Expected to be Implemented at Zendesk	
Applicable Trust Services Criteria	CSOCs
CC6.8	Antivirus and/or malware software have been implemented to prevent or detect the introduction of unauthorized or malicious software.
CC7.2	Vulnerability scans and penetration testing are performed periodically to identify vulnerabilities threatening the systems.
CC7.3, 7.4, 7.5	Incident Response Procedures are established and implemented to identify, analyze, and remediate potential security, availability, and confidentiality events and/or incidents.
CC8.1	SDLC has been established and implemented to ensure system changes are authorized, tested, and approved prior to production deployment.
	Policies and procedures for SDLC or infrastructure changes have been established and reviewed and are updated periodically.
	Procedures are implemented to identify deficiencies in the system and to ensure secured change management procedures are tracked and monitored.

Complementary Controls at User Entities

The Company's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the principal service commitments and system requirements related to the Company's services to be solely achieved by the Company's control procedures. Accordingly, user entities, in conjunction with the GovSlack system and related services, should establish their own internal controls or procedures to complement those of the System.

The following complementary user entities controls should be implemented by user entities to provide additional assurance that the applicable trust services criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent to user entities, user entities should exercise judgment in selecting and reviewing these complementary user entity controls.

#	Control Activities Expected to be Implemented at User Entities	Related Applicable Trust Services Criteria
1.	User entities are responsible for informing Slack of any regulatory issues that may affect the services provided by the System.	CC6.1; A1.2
2.	User entities are responsible for understanding and complying with their contractual obligations to Slack.	CC2.2, CC2.3, CC6.1; A1.2
3.	User entities are responsible for keeping the technical, billing, and administrative contact information on file with Slack up to date.	CC2.2, 2.3
4.	User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize the System.	A1.2, 1.3
5.	User entities are responsible for configuring the System security settings appropriately for the user entity.	CC6.1, CC6.3, CC6.6
6.	User entities are responsible for ensuring the confidentiality of any user accounts and passwords assigned to them for use with the System.	
7.	User entities are responsible for inviting new users to sign up for an account in the System, as well as removing terminated user accounts from the System.	

#	Control Activities Expected to be Implemented at User Entities	Related Applicable Trust Services Criteria
8.	User entities are responsible for ensuring that entity profile information stored by the System is accurate and complete.	CC6.1, CC6.3, CC6.6
9.	User entities are responsible for immediately notifying Slack of any actual or suspected information security breaches, including compromised user accounts.	CC7.3, CC7.4, CC7.5
10.	User entities are responsible for ensuring the appropriateness of designated Slack Workspace owner(s) and administrator(s).	CC6.1, CC6.3, CC6.6
11.	User entities are responsible for providing accurate and complete contact information to Slack for end users to be provisioned.	
12.	User entities are responsible for accepting the terms and agreement for utilizing Slack's services.	CC2.2, CC2.3
13.	User entities are responsible for monitoring and enforcing organizational compliance to Slack's terms and agreements.	
14.	User entities are responsible for configuring the message retention settings appropriately for the organization.	CC6.1; C1.1, C1.2
15.	User entities are responsible for developing and implementing their own information classification policies to govern sharing Personally Identifiable Information (PII) and other sensitive data in the System.	CC6.1, CC8.1

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security, availability, and confidentiality categories are applicable to the GovSlack Team Collaboration Platform system.