



A-ALIGN



Fallacy Labs, dba Slab, Inc.
SOC 3
2021

slab

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

May 1, 2021 to July 31, 2021

Table of Contents

SECTION 1 ASSERTION OF FALLACY LABS, DBA SLAB, INC. MANAGEMENT	1
SECTION 2 INDEPENDENT SERVICE AUDITOR’S REPORT	3
SECTION 3 FALLACY LABS, DBA SLAB, INC.’S DESCRIPTION OF ITS TEAM KNOWLEDGE SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD MAY 1, 2021 TO JULY 31, 2021	7
OVERVIEW OF OPERATIONS	8
Company Background	8
Description of Services Provided	8
Principal Service Commitments and System Requirements.....	8
Components of the System.....	8
Boundaries of the System.....	11
Changes to the System in the Last 12 Months.....	12
Significant Incidents in the Last 12 Months	12
Criteria Not Applicable to the System	12
Subservice Organizations	12
COMPLEMENTARY USER ENTITY CONTROLS	13

SECTION 1

ASSERTION OF FALLACY LABS, DBA SLAB, INC. MANAGEMENT

ASSERTION OF FALLACY LABS, DBA SLAB, INC. MANAGEMENT

August 23, 2021

We are responsible for designing, implementing, operating, and maintaining effective controls within Fallacy Labs, dba Slab, Inc.'s ('Slab' or 'the Company') Team Knowledge Software Services System throughout the period May 1, 2021 to July 31, 2021, to provide reasonable assurance that Slab's service commitments and system requirements relevant to Security (applicable trust services criteria) were achieved. Our description of the boundaries of the system is presented below in "Fallacy Labs, dba Slab, Inc.'s Description of Its Team Knowledge Software Services System throughout the period May 1, 2021 to July 31, 2021" and identifies the aspects of the system covered by our assertion.

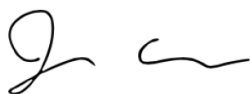
We have performed an evaluation of the effectiveness of the controls within the system throughout the period May 1, 2021 to July 31, 2021, to provide reasonable assurance that Slab's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Slab's objectives for the system in applying 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 "Fallacy Labs, dba Slab, Inc.'s Description of Its Team Knowledge Software Services System throughout the period May 1, 2021 to July 31, 2021".

Slab uses Google Cloud Platform ('GCP') to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Slab, to achieve Slab's service commitments and system requirements based on the applicable trust services criteria. The description presents Slab's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Slab's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary to achieve Slab's service commitments and system requirements based on the applicable trust services criteria. The description presents the applicable trust services criteria and the complementary user entity controls assumed in the design of Slab's controls.

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 May 1, 2021 to July 31, 2021 to provide reasonable assurance that Slab's service commitments and system requirements were achieved based on the applicable trust services criteria.



Jason Chen
Chief Executive Officer / Co-Founder
Fallacy Labs, dba Slab, Inc.

SECTION 2
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Fallacy Labs, dba Slab, Inc.:

Scope

We have examined Fallacy Labs, dba Slab, Inc.'s ('Slab' or 'the Company') accompanying description of its Team Knowledge Software Services System titled "Fallacy Labs, dba Slab, Inc.'s Description of Its Team Knowledge Software Services System throughout the period May 1, 2021 to July 31, 2021" (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 May 1, 2021 to July 31, 2021, to provide reasonable assurance that Slab's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Slab uses GCP to provide cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Slab, to achieve Slab's service commitments and system requirements based on the applicable trust services criteria. The description presents Slab's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Slab's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Slab, to achieve Slab's service commitments and system requirements based on the applicable trust services criteria. The description presents Slab's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Slab's controls. 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

Slab 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 Slab's service commitments and system requirements were achieved. Slab has provided the accompanying assertion titled "Assertion of Fallacy Labs, dba Slab, Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Slab 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
- 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.

Opinion

In our opinion, management's assertion that the controls within Slab's Team Knowledge Software Services System were suitably designed and operating effectively throughout the period May 1, 2021 to July 31, 2021, to provide reasonable assurance that Slab's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

The SOC logo for Service Organizations on Slab's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of Slab, user entities of Slab's Team Knowledge Software Services during some or all of the period May 1, 2021 to July 31, 2021, business partners of Slab subject to risks arising from interactions with the Team Knowledge Software Services, and those who have sufficient knowledge and understanding of the complementary user entity controls and 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.

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

A-LIGN ASSURANCE

Tampa, Florida
August 23, 2021

SECTION 3

FALLACY LABS, DBA SLAB, INC.'S DESCRIPTION OF ITS TEAM KNOWLEDGE SOFTWARE SERVICES SYSTEM THROUGHOUT THE PERIOD MAY 1, 2021 TO JULY 31, 2021

OVERVIEW OF OPERATIONS

Company Background

Slab was founded in August 2016, to help organizations share and retain long-term knowledge. Slab serves customers ranging from large enterprises to small startups, from diverse industries, such as high technology, consumer e-commerce, and healthcare.

Slab maintains its headquarters in San Francisco, California.

Description of Services Provided

Slab is an internal knowledge base that enables customers to collaboratively create, edit, organize and search content, with flexible organization and relevant search for later discovery and retrieval.

Slab is a web-based application provided through a software-as-a-service subscription model.

Principal Service Commitments and System Requirements

Slab designs its processes and procedures to securely steward its customer's internal knowledge while providing a reliable and feature rich product. Such processes and procedures are formally established, maintained, and updated in its Information Security Management System ('ISMS'). The policies identify functional responsibilities for the administration of logical access and security. Policies are regularly reviewed and approved no less than annually by Slab management.

Security commitments to user entities are documented and communicated in Service Level Agreements ('SLAs') and other customer agreements, as well as in the description of services offered online.

In addition, Slab systematically pursues independent assurance of ISMS controls through third-party assessments. These activities provide an independent assessment of risk management content and processes by performing periodic security assessments and compliance audits or examinations.

Components of the System

Infrastructure

Primary infrastructure used to provide Slab's Team Knowledge Software Services includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
Google Compute Platform	Compute, Load Balancer, SQL, Storage	Provides infrastructure and platform to host and deliver Slab software. Slab does not maintain its own hardware infrastructure

Software

Primary software used to provide Slab's Team Knowledge Software Services system includes the following:

Primary Software	
Software	Purpose
Algolia	Provides search indexing and ranking service
AppSignal	Provides application monitoring and error reporting

Primary Software	
Software	Purpose
Atlassian Statuspage	Provides application customer accessible application uptime status communication
Cloudflare	Provides static asset caching and content delivery network and static asset caching
GitHub	Provides code version control and issue tracking
Google Container Registry	Provides application image snapshot and deployment
Google Docs	Provides redundant copy of business continuity and incident response playbooks
Google Stackdriver	Provides application, infrastructure, database, audit logging and monitoring
Netlify	Provides marketing website hosting
PagerDuty	Provides application incident response notification and resolution tracking
Postmark	Provides transactional e-mail delivery service
Sentry	Provides application error reporting and tracking
Slab	Provides internal documentation and content management
Slack	Provides company-wide communication and real-time notifications
SolarWinds Pingdom	Provides application uptime monitoring
Retool	Provides user data administrative functions

People

The Slab staff provides support for its services in each of the following functional areas:

- Security Team: Responsible for guidance, direction, and authority for information security activities
- Incident Response Team: Responsible for investigating and responding to security related incidents
- Service Reliability Team: Responsible for day-to-day operations and maintenance of Slab services and investigating and addressing service availability and reliability related incidents
- Engineering Team: Responsible for the development of Slab's proprietary products and services
- Customer Success Team: Responsible for proactively engaging and responding to customers, resolving issues, soliciting feedback, or assisting in fully utilizing Slab's product offerings
- Legal Team: Responsible for human resources functions, onboarding and offboarding, and disciplinary actions for workforce members involved in privacy and security incidents

Data

Data, as defined by Slab, constitutes, but is not limited to, the following:

- System files
- Output reports
- Input reports
- Error logs
- Interaction data

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements established within Slab's ISMS. Slab has been specifically designed to protect sensitive customer data. The ISMS define the necessary policies and procedures used to protect data.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. All teams are expected to adhere to the Slab policies and procedures that define how services should be delivered. These are located on the Company's intranet and can be accessed by any Slab team member.

Physical Security

Slab relies on GCP's extensive experience in designing, constructing, and operating large-scale data centers for physical security and environmental protection of its infrastructure.

Logical Access

Slab employee and contractor user accounts are added, modified, or disabled in a timely manner and are reviewed on a periodic basis. In addition, password and multi-factor configuration settings for user authentication to Slab systems are managed in compliance with Slab's identity and access management procedures.

All resources are managed in the asset inventory system and each asset is assigned an owner. Owners are responsible for approving access to the resource and for performing periodic reviews of access by role.

Computer Operations - Backups

Slab utilizes an automated backup system to perform constant replication backups of application data. Each snapshot can be restored such that the database would be returned to a point in time in the past in the event that a rollback is necessary.

Computer Operations - Availability

Slab conducts regular business continuity planning, training, and testing. Business continuity and incident response plans and playbooks are maintained and updated to reflect new risks and lessons learned by past incidents and industry best practices. Slab's entire business continuity and incident response framework is reviewed and re-approved by senior management no less than annually.

Slab monitors the capacity utilization of computing infrastructure to ensure that service delivery matches SLAs. Slab evaluates the need for additional infrastructure capacity in response to growth of existing customers and/or the addition of new customers. Infrastructure capacity monitoring includes, but is not limited to:

- Instance compute utilization
- Instance memory utilization
- Database storage capacity
- File storage capacity
- Network bandwidth and latency

Change Control

Slab maintains documented Software Development Lifecycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. The goal of such policies and procedures is to prevent unintended service disruptions and maintain the integrity of service to the customer.

An issue tracker is utilized to document the change control procedures for changes in the application and implementation of new changes. Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Prior to deployment to production environments, changes are:

- Developed in a development environment that is segregated from the production environment
- Reviewed by peers for technical aspects and appropriateness
- Tested to confirm the changes will behave as expected when applied and not adversely impact. Whenever possible automated tests are included to supplement the continuous integration test suite

Production deployments are closely monitored for unintended impacts, such as high CPU or RAM usage, application errors, disk consumption, host failure, etc. Rollback procedures are documented so changes can be rolled back to the previous state if needed.

Data Communications

Firewall systems are in place to filter unauthorized inbound network traffic from the Internet and deny any type of network connection that is not explicitly authorized. Administrative access to the firewall is restricted to authorized employees.

Redundancy is built into the system infrastructure supporting the data center services to help ensure that there is no single point of failure that includes servers, databases, and routers. In the event that a primary system fails, the redundant infrastructure is configured to take its place.

Penetration testing is conducted to measure the security posture of a target system or environment. The third-party vendor uses an accepted industry standard penetration testing methodology, such as a Standard Grey Box Assessment Methodology. Once vulnerabilities are identified and confirmed, they are tracked and prioritized to their resolution.

Vulnerability scanning is performed on a regular basis, no less than monthly, in accordance with Slab policy. Scanning technologies are customized to test the organization's infrastructure and software in an efficient manner while minimizing the potential risks associated with active scanning. Scans are performed during non-peak windows.

Authorized employees may access the system through from the Internet through the use of in transit encryption, such as Secure Socket Layer ('SSL'), Virtual Private Network ('VPN'), or secure tunneling.

Boundaries of the System

The scope of this report includes the Team Knowledge Software Services System performed at the San Francisco, California facility.

This report does not include the cloud hosting services provided by GCP.

Changes to the System in the Last 3 Months

No significant changes have occurred to the services provided to user entities in the 3 months preceding the end of the review period.

Significant Incidents in the Last 3 Months

No significant incidents have occurred to the services provided to user entities in the 3 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common criterion was applicable to the Team Knowledge Software Services System at the San Francisco, California facilities.

Subservice Organizations

This report does not include the cloud hosting services provided by GCP at multiple facilities.

Subservice Description of Services

GCP provides cloud hosting services for Slab.

Complementary Subservice Organization Controls

Slab's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Slab's services to be solely achieved by Slab control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Slab.

The following subservice organization controls should be implemented by GCP to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - GCP		
Category	Criteria	Control
Common Criteria/Security	CC6.4, CC7.2	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge readers, biometric identification mechanisms, and/or physical locks.
		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of their visit.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a periodic basis and inappropriate access is removed in a timely manner.

Subservice Organization - GCP		
Category	Criteria	Control
		Data centers are continuously staffed and monitored by security personnel through the use of real-time video surveillance and/or alerts generated by security systems.
	CC4.1, CC6.6, CC6.7, CC7.1, CC7.2,	Monitoring tools send automated alerts to operational personnel based on predetermined criteria. Incidents are escalated per policy.
		The organization provides monitoring tools to relevant personnel to facilitate the detection and reporting of operational issues.

Slab's management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as SLAs. In addition, Slab performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing attestation reports over services provided by vendors and subservice organization
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

COMPLEMENTARY USER ENTITY CONTROLS

Slab'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 Trust Services Criteria related to Slab's services to be solely achieved by Slab control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Slab's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligations to Slab.
2. User entities are responsible for notifying Slab of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Slab services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Slab services.
6. User entities are responsible for providing Slab with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Slab of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.