JOHANSON GROUP

System and Organization Controls (SOC) 3

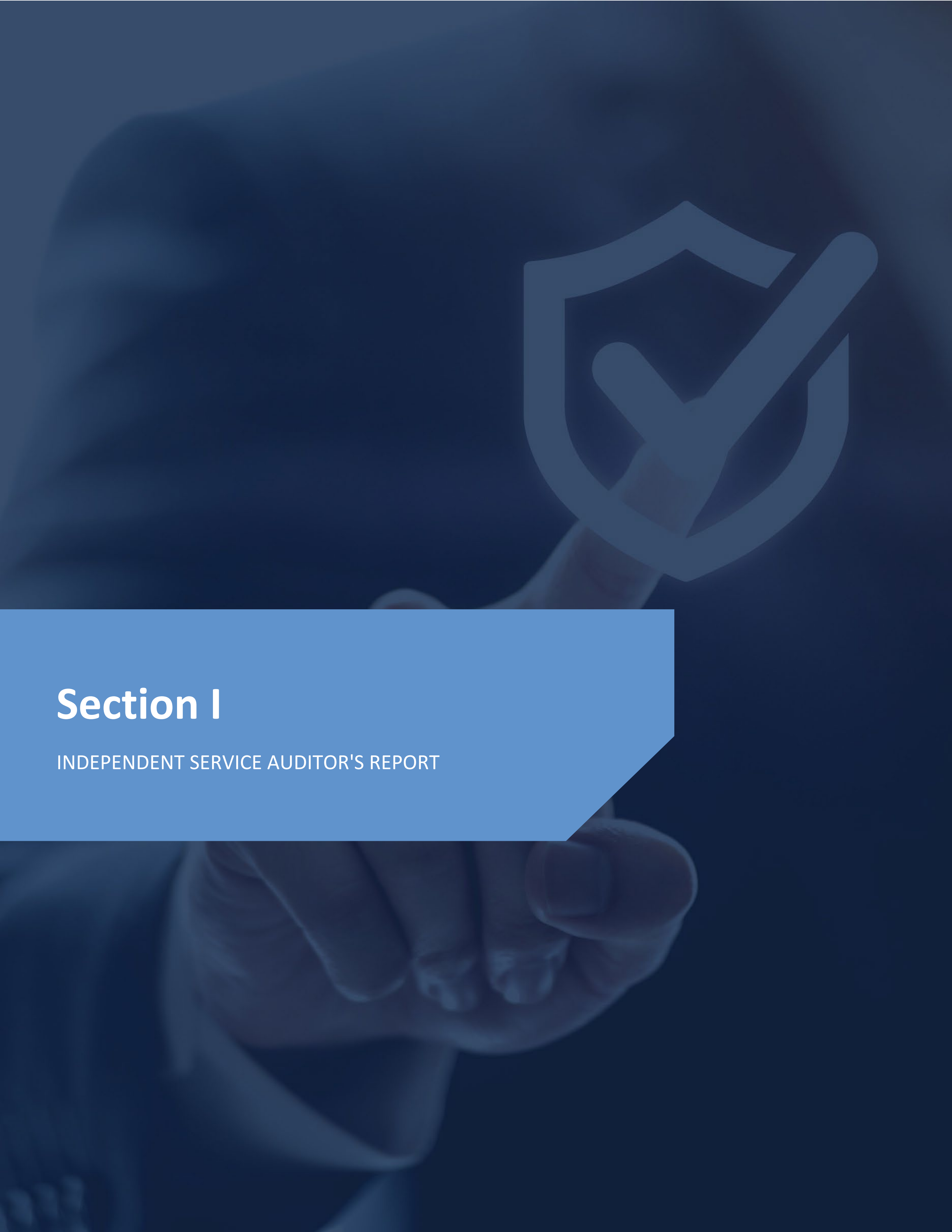
Relevant to the Trust Services Criteria for
Security

For the Period
August 01, 2024 to July 31, 2025

Together with Independent Service
Auditor’s Report

slab

TABLE OF CONTENTS



Section I

INDEPENDENT SERVICE AUDITOR'S REPORT

Slab

Scope

We have examined Slab's accompanying assertion titled "Assertion of Slab Management" (assertion) that the controls within Slab's Slab Team Knowledge Software (system) were effective throughout the period August 01, 2024 to July 31, 2025, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

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 also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, Slab is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 in achieving Slab'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 in achieving Slab'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 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.

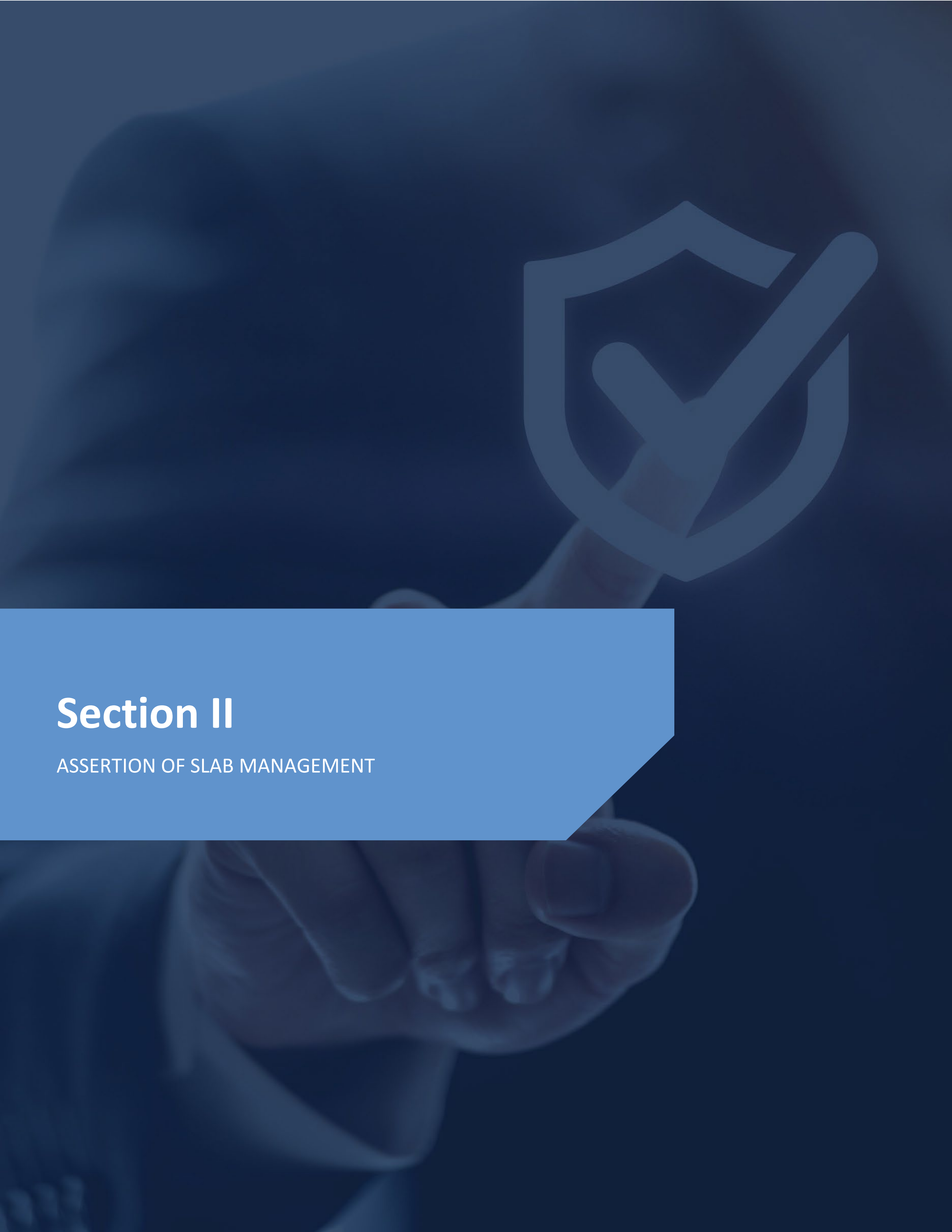
Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the 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 Slab's Slab Team Knowledge Software were effective throughout the period August 01, 2024 to July 31, 2025, to provide reasonable assurance that Slab service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

JohansonGroup LLP

Colorado Springs, Colorado
December 16, 2025



Section II

ASSERTION OF SLAB MANAGEMENT

We are responsible for designing, implementing, operating, and maintaining effective controls within Slab's Slab Team Knowledge Software (system) throughout the period August 01, 2024 to July 31, 2025, to provide reasonable assurance that Slab’s service commitments and system requirements relevant to security were achieved. Our description of the boundaries of the system is presented in the section of this report titled, “Description of Slab Team Knowledge Software” 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 August 01, 2024 to July 31, 2025, 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 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Slab'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 the accompanying system description.

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 August 01, 2024 to July 31, 2025, to provide reasonable assurance that Slab's service commitments and system requirements were achieved based on the applicable trust services criteria.

Slab Management
December 16, 2025

Section III

DESCRIPTION OF SLAB TEAM KNOWLEDGE SOFTWARE

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 is a remote company incorporated in California.

DESCRIPTION OF SERVICES OVERVIEW OR 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 customers' 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

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

The primary infrastructure used to provide Slab's Team Building Software Services system includes the following:

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

Software

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

Primary Software	
System/Application	**Purpose**
Algolia	Provides search indexing and ranking service
Instatus	Provides application customer accessible application uptime status communication
Cloudflare	Provides static asset caching and content delivery network and marketing website hosting
GitHub	Provides code version control and issue tracking
Google Container Registry	Provides application image snapshot and deployment
Google Docs	Provides a redundant copy of business continuity and incident response playbooks
Google Cloud Operations Suite	Provides application, infrastructure, database, audit logging, and monitoring
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

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 off-boarding, 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 following 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 defines the necessary policies and procedures used to protect data.

PROCESSES 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 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 Google's extensive experience in designing, constructing, and operating large-scale data centers for the physical security and environmental protection of its infrastructure.

Logical Access

Slab employee and contractor user accounts are added, modified, or disabled promptly and are reviewed periodically. 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 if 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 the 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 Management

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.

Before 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. If 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 for resolution.

Vulnerability scanning is performed regularly, no less than monthly, per Slab policy. Scanning technologies are customized to test the organization's infrastructure and software efficiently while minimizing the potential risks associated with active scanning. Scans are performed during non-peak windows.

Authorized employees may access the system from the Internet through the use of in-transit encryption, such as SSL, VPN, or secure tunneling.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the Team Knowledge Software services system performed in the San Francisco, California, facility.

This report does not include the Cloud Hosting and Infrastructure services provided by GCP.

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to all Security Category)
Security refers to the protection of i. Information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security preventor detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

CONTROL ENVIRONMENT

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Slab's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the products of Slab's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel
- Policies and procedures require employees to sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties, is a component of the employee handbook

Commitment to Competence

Slab has defined key formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs professionally and competently. Slab determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee performance periodically to determine that performance meets or exceeds Slab's standards.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements
- Training is provided to maintain the skill level of personnel in certain positions

Management's Philosophy and Operating Style

Slab's management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, and management's attitudes toward information processing, accounting functions, and personnel.

Specific control activities that the service organization has implemented in this area are described below:

- Executive management meetings are held to discuss major initiatives and issues that affect the business as a whole
- The entire team participates in a weekly all-heads meeting to review progress toward goals and discuss any major new announcements

Organizational Structure and Assignment of Authority and Responsibility

Slab's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Slab's assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility
- Organizational charts are communicated to employees and updated as needed
- Specific control activities that the service organization has implemented in this area are described below

Human Resource Policies and Practices

Slab's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensures the service organization is operating at maximum efficiency. Slab's policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment
- Evaluations for each employee are performed on an annual basis
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist

RISK ASSESSMENT PROCESS

Slab manages risk according to a formal risk management policy and supporting processes, including risk assessment.

There are some circumstances in which an information security risk assessment should be carried out, and these will vary in scope. In general, these are as follows:

- When the ISMS is launched
- When Slab management conducts an ISMS governance review
- As part of projects that involve a significant change to Slab, the ISMS, or its information assets
- When there have been major external changes affecting Slab, e.g., changes to relevant legislation, regulations, etc.
- If there is uncertainty regarding whether a risk assessment is appropriate, Slab will err on the side of caution and carry one out.

In summary, the risk assessment process proceeds as follows:

- Identification of Risks
- Risk Analysis and Evaluation
- Risk Treatment
- Selection of Controls

- Management Approval
- Risk Monitoring and Reporting
- Regular Review

Integration with Risk Assessment

The environment in which the system operates, the commitments, agreements, and responsibilities of Slab's Team Knowledge Software systems, as well as the nature of the components of the system, result in risks that the criteria will not be met. Slab addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Slab's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEMS

Information is necessary for Slab to carry out internal control responsibilities in support of the achievement of its objectives.

Communication occurs both internally and externally and provides the organization with the information needed to carry out day-to-day controls. Communication enables personnel to understand internal control responsibilities and their importance to the achievement of the objective.

Slab uses a variety of communication methods to ensure that significant events and issues are conveyed on time and that staff understand their role and responsibility concerning service delivery and controls. These methods include new hire training, ongoing training, policy and process updates, weekly departmental meetings summarizing events and changes, company-wide meetings, use of e-mail to communicate time-sensitive information, instant messaging, and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication within, as well as with customers.

MONITORING CONTROLS

Management monitors control to ensure that they are operating as intended and that controls are modified as conditions change. Slab's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Slab's management conducts quality assurance monitoring regularly, and additional training is provided based on the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management’s close involvement in Slab’s operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control’s weakness is made based on whether the incident was isolated or requires a change in the company’s procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Slab’s personnel.

On-Going Monitoring

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately.

Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Reporting Deficiencies

An internal tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool.

Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All relevant trust services criteria were applicable Slab Team Knowledge Software's.

SUBSERVICE ORGANIZATIONS

This report does not include the Cloud Hosting and Infrastructure services provided by GCP.

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's 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:

Category	Criteria	Control
Subservice Organization Controls - INSERT NAME OF SUBSERVICE ORG HERE		
Common Criteria/Security	CC6.4	User access lists to data center server areas are reviewed on a quarterly basis and inappropriate access is removed in a timely manner.
		All visitors must be escorted by an entity employee when visiting facilities where sensitive system and system components are maintained and operated.
		Visitors must be signed in by an employee before a single-day paper visitor badge that authorizes them can be issued.
		Annual datacenter security reviews are performed and results are reviewed by executive management.
		Physical security measures in place include:

Category	Criteria	Control
		• The existence of security guards, access badges, and video cameras to secure the data centers is reviewed during the annual data center security reviews • Data center entrances have a perimeter security system consisting of badge readers or biometric access system • Data centers utilize a badge reader or biometric access controls to restrict access to raised floor spaces and lock/keys to restrict access to facilities rooms within the building • All emergency exit points from the raised floor are alarmed • Badge reader and biometric access control systems are secured in a restricted space and no physical access to them from public spaces exists • Visitors to the data center facilities must gain appropriate approval, sign in at the front, and remain with an escort during the duration of their visit • Video cameras exist to monitor building entrances, exits, and the areas immediately surrounding the building • At least one security guard is on-site 24x7 • All staff members are required to either sign in or badge in to gain access to the facility and a no tailgating policy is in place • All Google cages, suites, and private rooms are secured using either lock/key, badge access control, or biometric access controls A key sign-out sheet and/or log of badge reader activity exists and covers access to Google spaces

Slab's management, along with the subservice organization, defines 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 and reconciling output reports
- Reviewing attestation reports over services provided by vendors and subservice organizations
- 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's control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Slab.

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 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 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.