INCREASE TECHNOLOGIES, INC.

SOC 2 REPORT

FOR

INCREASE PLATFORM

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

JULY 1, 2023, TO DECEMBER 31, 2023

Attestation and Compliance Services

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

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

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

TABLE OF CONTENTS

Section I

Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To Increase Technologies, Inc.:

Scope

We have examined Increase Technologies, Inc.'s ("Increase" or the "service organization") accompanying description of its Increase Platform, in Section 3, throughout the period July 1, 2023, to December 31, 2023, (the "description"), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period July 1, 2023, to December 31, 2023, to provide reasonable assurance that Increase'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, *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Increase uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Increase to achieve Increase's service commitments and system requirements based on the applicable trust services criteria. The description presents Increase's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Increase'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.

Service Organization's Responsibilities

Increase 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 Increase's service commitments and system requirements were achieved. Increase has provided the accompanying assertion, in Section 2, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. Increase 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 (AICPA) and in accordance with International Standard on Assurance Engagements 3000 (Revised), Assurance Engagements Other Than Audits or Reviews of Historical Financial Information, issued by the International Auditing and Assurance Standards Board. 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.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA and the International Ethics Standards Board for Accountants' Code of Ethics for Professional Accountants.

We applied the Statements on Quality Control Standards established by the AICPA and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

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

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

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

Description of Test of Controls

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

Opinion

In our opinion, in all material respects:

a. the description presents Increase's Platform system that was designed and implemented throughout the period July 1, 2023, to December 31, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period July 1, 2023, to December 31, 2023, to provide reasonable assurance that Increase's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of Increase's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period July 1, 2023, to December 31, 2023, to provide reasonable assurance that Increase's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Increase's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Increase; user entities of Increase's Platform system during some or all of the period of July 1, 2023, to December 31, 2023, business partners of Increase subject to risks arising from interactions with the Increase Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Schellman & Company, LLC

Tampa, Florida
January 26, 2024

SECTION 2

MANAGEMENT'S ASSERTION

Management's Assertion

We have prepared the accompanying description of Increase's Platform system, in Section 3, throughout the period July 1, 2023, to December 31, 2023, (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria"). The description is intended to provide report users with information about the Increase Platform system that may be useful when assessing the risks arising from interactions with Increase's system, particularly information about system controls that Increase has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security ("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)*.

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

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

a. the description presents Increase's Platform system that was designed and implemented throughout the period July 1, 2023, to December 31, 2023, in accordance with the description criteria;

b. the controls stated in the description were suitably designed throughout the period July 1, 2023, to December 31, 2023, to provide reasonable assurance that Increase's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations applied the complementary controls assumed in the design of Increase's controls throughout that period; and

c. the controls stated in the description operated effectively throughout the period July 1, 2023, to December 31, 2023, to provide reasonable assurance that Increase's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization assumed in the design of Increase's controls operated effectively throughout that period.

SECTION 3

DESCRIPTION OF THE SYSTEM

Overview of Operations

Company Background

Increase Technologies, Inc. (Increase) offers developer tools that enable companies to access banking services efficiently.

Description of Services Provided

Increase offers a cloud-based application programming interface (API) and dashboard that helps developers add banking capabilities to their websites or software applications (the "Increase Platform"). The Increase Platform enables end users to spin up bank accounts, create cards, initiate funds transfers, and retrieve account activity data.

Increase customers are primarily businesses that use the Increase services for their corporate business banking needs and/or to enable banking capabilities, such as money movement or money storage, for their customers.

Increase is not a bank. In some cases, Increase is a program manager to its bank partners who contract with Increase customers to provide the regulated depository account services. Banks use Increase to retrieve data related to the bank customer's account activity for internal and external reporting purposes.

Principal Service Commitments and System Requirements

Principal Service Commitments

The Increase' service terms, description of the service offered, and related documentation describe Increase's service commitments to customers about the performance of the Increase platform. The service commitments are designed to meet Increase's objectives in compliance with applicable laws and regulations. System requirements for security are contained in Increase policies and procedures and specify how Increase meets its service commitments.

Standard security service commitments include using organizational, technical, and administrative controls to protect customer information from unauthorized access or loss.

Increase's security system commitments include:

- System access is granted to authorized personnel only
- Protection of data at rest and in transit
- Regular security assessments
- Identification and remediation of security incidents/events
- Regular system updates
- An information security program is designed to protect the security, integrity, and confidentiality of the system and its information
- Risk assessments for both internal and external threats to the system and its information

Increase's system requirements for security include:

- Use of end-to-end encryption to protect confidential data at rest and in transit
- Role based security capabilities to restrict access to data

- Employee provisioning and deprovisioning standards
- Intrusion detection standards
- Risk and vulnerability management standards
- Incident handling standards
- Change management standards
- Vendor management

System Requirements

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

Components of the System Used to Provide the Service

System Boundaries

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

Infrastructure and Software

Google Cloud Platform (GCP) is a cloud infrastructure provider and solutions partner to support scalability, availability, and durability of the platform and services. Increase is hosted in Google Cloud region us-west1 (Oregon), located in the United States of America. Increase receives assistance from Google Cloud technical account managers who assist with support issues.

GCP and Increase share responsibility for system security. Increase chooses which security capabilities to implement to protect customer data, platform, application systems, operating systems, encryption keys, and networks. GCP provides security at the infrastructure layer, where Increase software and data are hosted, for components such as computing, storage, database, and networking building blocks (i.e., responsible for security of the cloud).

The in-scope infrastructure consists of multiple applications, as shown in the table below:

Primary Infrastructure			
Production System	**Business Function Description**	**Operating System Platform**	**Physical Location**
Google Compute Engine (GCE), Google Kubernetes Engine (GKE)	Compute services for creating and running virtual machines.	GCP Proprietary	GCE (US-west1)
Google Container Registry (GCR)	Repository for storing container images.		

Primary Infrastructure			
Production System	Business Function Description	Operating System Platform	Physical Location
Firewalls	Google Cloud Virtual Private Cloud (VPC) firewall rules configured within the GCP Console allow Increase the ability to configure, control, and restrict inbound and outbound network traffic into the production infrastructure.	GCP Proprietary	GCE (US-west1)
Databases	Production databases supporting the Increase services and systems.	Google Cloud SQL	

In addition, Increase utilizes the following systems to support the Increase Platform:

- Google Admin – access management tool utilized to manage Google Workspace services
- Google Identity and Access Management (IAM) – provision access to certain production resources (e.g., GCP Console).
- GitHub – version control software utilized to control access to source code and provide roll back capabilities for application and infrastructure changes.
- GitHub Actions – automated software deployment workflow from within GitHub.
- GitHub Dependabot – automated pull request tool to help update dependencies with known vulnerabilities.
- Asana – ticketing system utilized for centrally managing and tracking production issues and change management activities.
- Google Cloud Platform Secret Manager – securely stores API keys, passwords, certificates, and other sensitive data.
- Google Cloud Monitoring and Logging – collects metrics, events, and metadata from GCP.
- Google Intrusion Detection System (IDS) – intrusion detection service that provides threat detection for intrusions, malware, spyware, and command-and-control attacks on the network.
- Slack – communications platform utilized to facilitate daily conversations related to various aspects of the business. Project channels are private groups restricted on a need-to-know basis.
- Dropbox – cloud-based document repository and document creation software.
- Terraform – infrastructure as a code tool used to build, change, and version cloud resources.

People

Separate departments are responsible for the Increase Platform security.

- Corporate – executives, senior operations staff, and Increase administration such as legal and compliance. Responsible for overseeing company-wide activities, establishing and accomplishing goals, and managing objectives.
- Customer experience – responsible for supporting users and administering day-to-day processes to facilitate the user experience.
- Engineering – responsible for software development, infrastructure monitoring, information security, system administration, systems development, and application support.

Procedures

Access, Authentication, and Authorization

The in-scope systems (e.g., Google Admin, production servers, databases, containers, GCP Console, etc.), are configured to authenticate users with a user account and enforce minimum password requirements and/or multi-factor authentication (MFA).

GCP firewalls are configured to filter inbound and outbound network traffic from the Internet and grant specific IP addresses the ability to establish remote connections to production servers. The web portal application connections to the Internet are encrypted via transport layer security (TLS) 1.3.

Administrative access privileges within each of the production systems (e.g., Google Admin, production servers, databases, containers, GCP Console, etc.) are restricted to user accounts accessible by authorized personnel. User access reviews are performed at least annually to help ensure that only authorized personnel maintain access to the production environment.

Additionally, the production network is segmented to help ensure that confidential data is isolated from other unrelated networks.

Access Requests and Access Revocation

Management has established controls to help ensure that access to data is restricted to those who require access. A formal process has been established for managing user accounts and controlling access to Increase's resources within the production environment. When a new employee is hired and has accepted a position at Increase, user access provisioning and onboarding requirements are documented as part of a standardized process.

Management notifies system administrators when employees are terminated. System administrators revoke user accounts assigned to terminated employees upon notification.

Change Management

Increase has a formalized change management process in place to provide a layer of protection by ensuring every change performed is tested to verify operational functionality and approved by the organization. Version control is utilized to track changes, record state, and aid in rollbacks. Program development and testing efforts are performed in distinct development and quality assurance (QA) environments that are logically separated from the production environment.

Proposed changes are categorized and assessed for the level of risk they pose to the system. Normal and time-sensitive changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and customer notifications, must be performed. Time-sensitive changes follow the formalized change management process, but at an accelerated timeline. Reviews of time-sensitive changes implemented to the production environment are performed on a bi-weekly basis to help ensure that only authorized changes were made to the system. Changes to system infrastructure are managed as code and follow the same change management processes as described.

Write and administrative access privileges to the version control software are restricted to user accounts accessible by authorized personnel. Access privileges to promote changes into the production environment are restricted to user accounts accessible by authorized development personnel.

The organization is notified of changes on a continuous basis to promote visibility into the system. The automated deployment tool is configured to alert engineering personnel via the internal team collaboration tool when deployments occur and when branch protection rules are disabled. A test suite is configured to run against the code to determine if a change meets the business objective and an automated patch management tool is in place to monitor for new patches to relevant systems. The deployment tool is configured to alert users when the branch protection is disabled.

Data Backup and Disaster Recovery (DR)

Increase performs data backup restoration tests at least annually to verify data reliability and information integrity. A documented business continuity (BC) / DR plan is in place and tested annually.

System Monitoring

Increase performs ongoing evaluations to ascertain whether the components of internal control are present and functioning. Internal personnel conduct periodic assessments and tests of internal controls that include (a) using a software application, which alerts management when internal control and security issues arise, to objectively and continuously monitor the Increase's control environment; (b) working with process owners and engineering personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed.

Increase leverages several tools to continuously address the security of the system, such continuous monitoring of code repositories to capture patches and automated scanning of live environments to detect unexpected behavior. Increase has an internal service-level agreement (SLA) for remediating vulnerabilities based on their severity categories. Annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and benchmark the environment against cybersecurity practices. The penetration testing scope is determined based on Increase's areas of risk and compliance requirements.

Incident Response

An incident response plan is documented to manage unexpected incidents that interrupt normal business functions. Reported or detected security incidents are tracked within an internal collaboration tool until resolved. Security incidents are reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved.

Data

Increase stores two types of data: Customer data and Card data.

Customer data is information about the user that Increase uses to provide the services. The data includes:

- Customer profile information collected at onboarding to satisfy bank and regulatory compliance requirements.
- Systems logs audit events for information security and possible future forensic analysis.
- User device metadata for fraud prevention.
- Customer bank details (account and routing number) for account funding.
- Transaction metadata from processing bank account activity.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with requirements formally established in customer contracts. Increase has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Customer data is kept confidential but is not subject to the technical security controls described below for Card data.

Card data is the 16-digit credit card number that Increase provides a user when they create a credit card. Card data is maintained in a secure database and is encrypted at rest and in transit. Card data is only decrypted locally on an end user device on an endpoint application or web browser.

Increase customers submit Customer data and transaction instructions to Increase via the dashboard or API. Front ends communicate to Increase servers over encrypted TLS connections.

Increase connects directly to sponsor banks, Visa, The Clearing House, and the Federal Reserve (the Networks).

Customer data is shared between Increase and sponsor banks, The Clearing House, and the Federal Reserve over encrypted Secure File Transfer Protocol.

Card data and associated transaction instructions are sent to Visa in the ISO 8583 protocol format over private fiber networks or encrypted Internet Protocol security tunnels.

Significant Changes During the Period

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

Subservice Organization

The cloud hosting services provided by Google were not included within the scope of this examination.

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

Control Activities Expected to be Implemented by Google	Applicable Trust Services Criteria
Google is responsible for ensuring data within GCP is stored in an encrypted at rest format.	CC6.1
Google is responsible for ensuring access to Cloud Storage server-side encryption keys is restricted to authorized personnel.	CC6.1
Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.	CC6.1 – CC6.3, CC6.5 – CC6.6
Google is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	CC6.4 – CC6.5
Google is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the Increase systems reside.	CC6.7
Google is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.	CC7.2

CONTROL ENVIRONMENT

The control environment at Increase is the foundation for the other areas of internal control. It sets the tone of the organization and influences the control consciousness of its personnel. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided the board of directors and audit compliance committee oversight.

Integrity and Ethical Values

Increase maintains trust by keeping promises, acting with honesty and integrity, and reaching company goals through appropriate conduct. Increase continuously evaluates practices and processes to ensure that Increase is upholding its ethical values and meeting the expectations of its stakeholders. 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 the control environment, affecting the design, administration, and monitoring of other components. Specific control activities that Increase has implemented in this area are described below.

- Increase employees sign an employment agreement that requires them to comply with company policies and procedures, which includes the employee handbook.
- Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage.
- Employees sign a confidentiality agreement upon hire. This agreement prohibits the disclosure of information and other data to which the employee has been granted access.
- Managers complete performance appraisals and give feedback on information security issues during annual performance reviews.
- Increase has documented processes for disciplinary actions for employees and contractors who violate the information security policy.
- New personnel offered employment are subject to background checks prior to their start date.
- Increase has a policy that requires that third party contractors and vendors are assessed for risk to Increase.
- Employees complete annual security awareness training.

Board of Directors and Audit and Compliance Committee Oversight

Increase is a founder-led company with a single board member. The board of directors has established bylaws and is responsible for the oversight of Increase.

Increase relies on a four-person audit and compliance committee that is responsible for ensuring the company is meeting its business objectives and remaining compliant. The audit and compliance committee establishes, communicates, and monitors control policies and procedures. The audit and compliance committee meets at least monthly to discuss information security, internal control, and operational activities.

Organizational Structure and Assignment of Authority and Responsibility

Increase has established lines of reporting that facilitate the flow of information to the appropriate personnel. Increase uses a centralized organizational model to support applications and technology. Increase has an organization chart that sets forth the lines of reporting and is updated as necessary. Roles and responsibilities are segregated based on functional requirements. The audit and compliance committee has documented oversight responsibilities relative to internal control and the implementation of security.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define an employee’s roles and responsibilities. Increase’s commitment to competence includes management consideration of the competence levels for particular jobs and how those levels translate in requisite skills and knowledge. Management ensures employees have adequate training to carry out their job responsibilities. Specific control activities that Increase has implemented in this area are described below.

- Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage.
- Employees complete annual security awareness training.
- Increase management conducts an annual talent review and succession planning session to ensure staffing levels are adequate for information security coverage to meet company objectives.
- Increase has a standard hiring and onboarding process for new employees. They are introduced to Increase’s policies, culture, tools, and processes during their first week.

- Job descriptions are documented for employees supporting the services and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.

Accountability

Management establishes accountability by setting a strong tone at the top and holding those accountable for internal control responsibilities. Management communicates the internal control responsibilities and the criteria that employees will be measured against as well as incentives and other rewards. Specific control activities that Increase has implemented in this area are described below.

- Managers complete performance appraisals and give feedback on information security issues during annual performance reviews. Managers record any feedback related to information security feedback.
- Increase employees sign an employment agreement that requires them to comply with company policies and procedures, which includes the employee handbook.
- Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage.
- Increase has documented processes for disciplinary actions for employees and contractors who violate the information security policy.
- Increase management meets annually to discuss employee compensation, including to evaluate any economic incentives that could create negative incentives for compliance with company information security.

Risk Assessment

Management is responsible for identifying the risks that threaten the organization's ability to provide reliable service for user entities. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them.

Objective Setting

Increase has a cross-functional risk assessment process that utilizes management and staff expertise to identify risks that could affect Increase's ability to meet its obligations to its customers. Risk assessment efforts include analyses of technical and non-technical threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Internal controls, policy, and procedure form the basis of risk mitigation. Exceptions or deferments are to be documented and must be approved by management of the group which originates or monitors the control in question.

Risk Identification and Analysis

Management meets at least bi-weekly to identify risks and develop corrective steps to minimize the impact of these risks. Increase employs numerous methods to assess and manage risk, including documentation, policies, procedures, team structure, recurring meetings, and automated error detection controls. Team members are instructed by general policy to relate suspected or confirmed risks to the engineering team for analysis, and mitigation as appropriate.

Risk Factors

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

External Factors

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

Internal Factors

- Significant changes in policies, processes, or personnel
- Types of fraud, fraud incentives, pressures, opportunities, attitudes, and rationalizations for employees
- A disruption in information systems processing
- The quality of personnel hired, and methods of training utilized
- Changes in management responsibilities

Potential for Fraud

Management considers the potential for fraud when assessing the risks to Increase's objectives. The potential for fraud can occur in both financial and non-financial reporting. Other types of fraud include the misappropriation of assets and illegal acts such as violations of governmental laws.

Management realizes that the potential for fraud can occur when employees are motivated by certain pressures or incentivized to commit fraud. The absence of controls, or ineffective controls, provides an opportunity for fraud when combined with an incentive to commit fraud. Therefore, management considers fraud factors in each risk evaluated during the risk assessment process.

Risk Mitigation

Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through a liability insurance policy. Management personnel are required to identify significant risks relating to their areas of responsibility and implement measures to mitigate those risks. The organization has documented policies and procedures to guide personnel throughout this process. The annual risk assessment and mitigation process also addresses risks arising from potential business disruptions.

Third parties are also considered during the annual risk assessment and mitigation process. Documented policies and procedures are in place to guide personnel in identifying risks associated with vendors and contractors as part of the risk assessment process.

Trust Services Criteria and Related Control Activities

Integration with Risk Assessment

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

Selection and Development of Control Activities

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

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

Trust Services Criteria Not Applicable to the In-Scope System

All criteria within the security category are applicable to the Increase Platform.

Information and Communication Systems

Information and communication are an integral component of Increase's internal controls. It is the process of identifying, capturing, and exchanging information in the form and timeframe necessary to conduct, manage, and control the entity's operations. At Increase, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, partners, and employees.

Internal Communications

Daily communication via instant messaging as well as calendared weekly and monthly calls/virtual meetings including scheduled team check-ins and standups are held by business units to share and discuss operational efficiencies within the applicable functional areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization.

External Communications

Increase has also implemented various methods of communication to help provide assurance that clients understand their roles and responsibilities in processing their transactions and communication of significant events. Increase utilizes the public-facing website to communicate relevant information regarding the design and operation of the system and Increase's commitments to external customers. The website also features a portal where customers can communicate with Increase for support of the system or to report any incidents or concerns related to the operation or security of the system.

Monitoring

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

Ongoing Monitoring

Increase performs ongoing evaluations to ascertain whether the components of internal control are present and functioning. Increase leverages several tools to continuously address the security of the system, such continuous monitoring of code repositories to capture patches and automated scanning of live environments to detect unexpected behavior. Increase has an internal SLA for remediating vulnerabilities based on their severity categories. The audit and compliance committee meets monthly to discuss information security, internal control, and operational activities.

Separate Evaluations

Internal personnel conduct periodic assessments and tests of internal controls that include (a) using a software application, which alerts management when internal control and security issues arise, to objectively and continuously monitor Increase's control environment; (b) working with process owners and information security personnel to identify specific security threats and vulnerabilities and how the associated risk is being addressed. Annual penetration tests are performed by an external service provider to identify specific technical threats and vulnerabilities and benchmark the environment against cybersecurity practices. The penetration testing scope is determined based on Increase's areas of risk and compliance requirements.

Subservice Organization Monitoring

Increase reviews available vendor System and Organization Controls (SOC) reports annually as part of the vendor risk assessment process.

Evaluating and Communicating Deficiencies

A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to Increase's objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.

Complementary Controls at User Entities

Increase's controls are designed to provide reasonable assurance that the principal service commitments and system requirements can be achieved without the implementation of complementary controls at user entities. As a result, complementary user entity controls are not required, or significant, to achieve the principal service commitments and system requirements based on the applicable trust services criteria.

SECTION 4

TESTING MATRICES

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to the Increase Platform system provided by Increase. The scope of the testing was restricted to the Increase Platform system and its boundaries as defined in Section 3. Schellman conducted the examination testing over the period July 1, 2023, to December 31, 2023.

Tests of Operating Effectiveness

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

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

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

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

Sampling

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

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

Reliability of Information Provided by the Service Organization

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

Test Results

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

Security Category

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	Increase employees sign an employment agreement that requires them to comply with company policies and procedures, which includes the employee handbook.	Inspected the listing of employees hired during the period with the assistance of the head of engineering and determined that there were no employees hired during the period, therefore, no testing of operating effectiveness was performed.	
CC1.1.2	Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage on an annual basis.	Inspected the information security policy attestation for a sample of current employees to determine that each company employee sampled reviewed and attested to their agreement with the information technology security policy that described their responsibilities and expected behavior, including regarding data and information system usage during the period.	No exceptions noted.
CC1.1.3	Employees sign a confidentiality agreement upon hire. This agreement prohibits the disclosure of information and other data to which the employee has been granted access.	Inspected the listing of employees hired during the period with the assistance of the head of engineering, and determined that there were no employees hired during the period, therefore, no testing of operating effectiveness was performed.	

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.1.4	Increase has a documented process for disciplinary actions for employees and contractors who violate the information security policy.	Inspected the employee handbook and the employee disciplinary action policies and procedures to determine that Increase had a documented process for disciplinary actions for employees and contractors who violated the information technology policy.	No exceptions noted.
CC1.1.5	New personnel offered employment are subject to background checks prior to their start date.	Inspected the listing of employees hired during the period with the assistance of the head of engineering, and determined that there were no employees hired during the period, therefore, no testing of operating effectiveness was performed.	
CC1.1.6	Increase has a policy that requires that third-party contractors and vendors are assessed for risk to Increase.	Inspected the third-party risk management policy to determine that Increase had a policy that required that third-party contractors and vendors were assessed for risk to Increase.	No exceptions noted.
CC1.1.7	Employees complete annual security awareness training.	Inspected the completed security awareness training documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	The audit and compliance committee oversees Increase information security practices.	Inspected the audit and compliance committee charter and the membership listing of the audit and compliance committee to determine that the audit and compliance committee oversaw Increase information security practices.	No exceptions noted.
CC1.2.2	The audit and compliance committee charter reflects the required skills to participate in the audit and compliance committee.	Inspected the audit and compliance committee charter and the membership listing of the audit and compliance committee to determine that the audit and compliance committee charter reflected the necessary skills to participate in the audit and compliance committee.	No exceptions noted.
CC1.2.3	The audit and compliance committee is composed of at least three Increase employees, including an expert in information technology, corporate compliance, and financial regulations.	Inspected the audit and compliance committee charter and the membership listing of the audit and compliance committee to determine that the audit and compliance committee was composed of at least three Increase employees, including an expert in financial technology, corporate compliance, and financial regulations.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.2.4	The audit and compliance committee is empowered to retain legal counsel and consultants as necessary for supplementing expertise.	Inspected the audit and compliance committee charter and the membership listing of the audit and compliance committee to determine that the audit and compliance committee was empowered to retain legal counsel and consultants as necessary for supplementing expertise.	No exceptions noted.
CC1.2.5	The audit and compliance committee meets monthly to discuss information security, internal control, and operational activities.	Inspected the recurring audit and compliance committee meeting invite and minutes during the period to determine that the audit and compliance committee met monthly to discuss IT, internal control, and operational activities.	No exceptions noted.
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	An organizational chart is documented and defines the organizational structure and reporting lines.	Inspected the organizational chart to determine that an organizational chart was documented and defined the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	The audit and compliance committee has documented oversight responsibilities relative to internal control and the implementation of security.	Inspected the audit and compliance committee charter to determine that management had documented oversight responsibilities relative to internal control and the implementation of security.	No exceptions noted.
CC1.3.3	Job descriptions are documented for employees supporting the services and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the documented job descriptions for a sample of employment positions to determine that job descriptions were documented for employees supporting the services and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage on an annual basis.	Inspected the information security policy attestation for a sample of current employees to determine that each company employee sampled reviewed and attested to their agreement with the information technology security policy that described their responsibilities and expected behavior, including regarding data and information system usage during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.4.2	Employees complete annual security awareness training.	Inspected the completed security awareness training documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC1.4.3	Increase management conducts an annual talent review and succession planning session to help ensure staffing levels are adequate for information security coverage to meet company objectives.	Inspected the most recent talent review and succession planning meeting invite and meeting notes to determine that company management conducted a talent review and succession planning session during the period to ensure staffing levels were adequate for information security coverage to meet company objectives.	No exceptions noted.
CC1.4.4	Increase has a standard hiring and onboarding process for new employees. They are introduced to Increase's policies, culture, tools, and processes during their first week.	Inspected the listing of employees hired during the period with the assistance of head of engineering, and determined that there were no employees hired during the period, therefore, no testing of operating effectiveness was performed.	
CC1.4.5	Job descriptions are documented for employees supporting the services and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the documented job descriptions for a sample of employment positions to determine that job descriptions were documented for employees supporting the services and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	Increase employees sign an employment agreement that requires them to comply with company policies and procedures, which includes the employee handbook.	Inspected the listing of employees hired with the assistance of the head of engineering and determined that there were no employees hired during the period, therefore, no testing of operating effectiveness was performed.	
CC1.5.2	Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage on an annual basis.	Inspected the information security policy attestation for a sample of current employees to determine that each company employee sampled reviewed and attested to their agreement with the information technology security policy that described their responsibilities and expected behavior, including regarding data and information system usage during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC1.5.3	Increase has a documented processes for disciplinary actions for employees and contractors who violate the information security policy.	Inspected the employee handbook and the employee disciplinary action policies and procedures to determine that Increase had a documented process for disciplinary actions for employees and contractors who violated the information technology policy.	No exceptions noted.
CC1.5.4	Increase management meets annually to discuss employee compensation, including to evaluate any economic incentives that could create negative incentives for compliance with company information security.	Inspected the most recent compensation meeting invite and minutes to determine that Increase management met during the period to discuss employee compensation, including to evaluate any economic incentives that could create negative incentives for compliance with company information security.	No exceptions noted.
Communication and Information			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	Data and information critical to the system is mapped and assessed annually for relevance and use.	Inspected the most recent data and information review and the related documentation to determine that data and information critical to the system was mapped and assessed for relevance and use during the period.	No exceptions noted.
CC2.1.2	Security vulnerabilities that are detected are triaged by the engineering team and monitored through resolution.	Inspected the remediation tickets for a sample of security vulnerabilities during the period to determine that each vulnerability sampled that was detected was triaged by the engineering team and monitored through resolution.	No exceptions noted.
CC2.1.3	Enterprise monitoring applications are in place to monitor the performance and availability of production servers and devices.	Inspected the monitoring applications configurations and example alerts generated during the period to determine that the following enterprise monitoring applications were in place to monitor the performance and availability of product servers and devices.	No exceptions noted.
CC2.1.4	Increase’s handbook contains a requirement for employees to maintain the security and confidentiality of system data.	Inspected the employee handbook to determine that Increase’s handbook contained a requirement for employees to maintain the security and confidentiality of system data.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.1.5	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage on an annual basis.	Inspected the information security policy attestation for a sample of current employees to determine that each company employee sampled reviewed and attested to their agreement with the information technology security policy that described their responsibilities and expected behavior, including regarding data and information system usage during the period.	No exceptions noted.
CC2.2.2	Job descriptions are documented for employees supporting the services and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the documented job descriptions for a sample of employment positions to determine that job descriptions were documented for employees supporting the services and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.
CC2.2.3	Employees complete annual security awareness training.	Inspected the completed security awareness training documentation for a sample of current employees to determine that each employee sampled completed security awareness training during the period.	No exceptions noted.
CC2.2.4	The audit and compliance committee meets monthly to discuss information security, internal control, and operational activities.	Inspected the recurring audit and compliance committee meeting invite and minutes during the period to determine that the audit and compliance committee met monthly to discuss IT, internal control, and operational activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.2.5	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan on the company intranet to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC2.2.6	Policies and procedures are communicated to employees on the compliance dashboard.	Inspected the compliance program dashboard on the company intranet to determine that policies and procedures were communicated to employees on the compliance dashboard.	No exceptions noted.
CC2.2.7	Changes to Increase's objectives are communicated to personnel during weekly meetings.	Inspected the business meeting invite and minutes for a sample of weeks during the period to determine that changes to Increase's objectives were communicated to personnel for each week sampled.	No exceptions noted.
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan and compliance program dashboard to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC2.3.2	A system description is documented that provides information regarding the design and operation of the system and its boundaries. The system description is communicated to external users via the company website.	Inspected the system description on the company's external website to determine that a system description was documented that provided information regarding the design and operation of the system and its boundaries and the system description was communicated to external users via the company website.	No exceptions noted.
CC2.3.3	Increase has made available contact e-mail on its website.	Inspected the company's external website to determine that Increase has made available contact e-mail on its website.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC2.3.4	Standard customer contracts are executed to define and communicate the security responsibilities of Increase and external users.	Inspected the executed customer contracts for a sample of customers onboarded during the period to determine that standard customer contracts were executed to define and communicate the security responsibilities of Increase and external users.	No exceptions noted.
CC2.3.5	The security commitments and obligations of vendors are documented and communicated via master service agreements or nondisclosure agreements.	Inspected the executed master service agreement for a sample of vendors to determine that the security commitments and obligations of vendors were documented and communicated via master service agreements or nondisclosure agreements for each vendor sampled.	No exceptions noted.
CC2.3.6	Increase has a policy that requires that third-party contractors and vendors are assessed for risk to Increase.	Inspected the third-party risk management policy to determine that Increase had a policy that required that third-party contractors and vendors were assessed for risk to Increase.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	Increase established organizational strategies and objectives that are used to determine entity structure and performance metrics.	Inspected the most recent audit and compliance committee meeting invite and minutes to determine that Increase established organizational strategies and objectives that were used to determine entity structure and performance metrics.	No exceptions noted.
CC3.1.2	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.1.3	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.2.2	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC3.2.3	Information security personnel conduct a technological risk assessment on an annual basis to identify technology risks across the entity and analyze risks as a basis for determining how the risks should be managed.	Inspected the most recently completed risk assessment documentation to determine that IT personnel conducted a technological risk assessment during the period to identify technology risks across the entity and analyzed risks as a basis for determining how the risks should be managed.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.2.4	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	Management conducts a fraud risk assessment as part of the annual risk assessment to identify the various ways that fraud and misconduct can occur.	Inspected the most recently completed risk assessment documentation to determine that management conducted a fraud risk assessment during the period to identify the various ways that fraud and misconduct could occur.	No exceptions noted.
CC3.3.2	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.3.3	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC3.3.4	Increase management meets annually to discuss employee compensation, including to evaluate any economic incentives that could create negative incentives for compliance with company information security.	Inspected the most recent compensation meeting invite and minutes to determine that Increase management met during the period to discuss employee compensation, including to evaluate any economic incentives that could create negative incentives for compliance with company information security.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC3.4.2	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC3.4.3	Increase has a policy that requires that third-party contractors and vendors are assessed for risk to Increase.	Inspected the third-party risk management policy to determine that Increase had a policy that required that third-party contractors and vendors were assessed for risk to Increase.	No exceptions noted.
CC3.4.4	Increase reviews available vendor SOC reports annually as part of the vendor risk assessment process.	Inspected the most vendor recent risk assessment documentation for a sample of vendors to determine that the company reviewed available vendor SOC reports as part of the vendor risk assessment process for each vendor sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC4.1.2	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC4.1.3	Increase reviews available vendor SOC reports annually as part of the vendor risk assessment process.	Inspected the most vendor recent risk assessment documentation for a sample of vendors to determine that the company reviewed available vendor SOC reports as part of the vendor risk assessment process for each vendor sampled.	No exceptions noted.
CC4.1.4	The audit and compliance committee meets monthly to discuss information security, internal control, and operational activities.	Inspected the recurring audit and compliance committee meeting invite and minutes during the period to determine that the audit and compliance committee met monthly to discuss IT, internal control, and operational activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC4.2.2	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC4.2.3	The audit and compliance committee meets monthly to discuss information security, internal control, and operational activities.	Inspected the recurring audit and compliance committee meeting invite and minutes during the period to determine that the audit and compliance committee met monthly to discuss IT, internal control, and operational activities.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A formal risk assessment is performed on an annual basis that considers the identification and assessment of risks relating to company objectives, including risks arising from potential business disruptions, vendors, and the potential for fraud. Identified risks are rated using a risk evaluation process that accounts for changes in risk from the prior year, and are formally documented, along with mitigation strategies, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC5.1.2	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.1.3	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the period and the control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	A risk assessment is performed on at least an annual basis that considers the identification and assessment of risks relating to Company objectives. Risks that are identified are rated using a risk evaluation process and are documented, along with remediation strategies and actions, for management review.	Inspected the most recently completed risk assessment documentation to determine that a formal risk assessment was performed during the period that considered the identification and assessment of risks related to company objectives, including risk arising from potential business disruptions, vendors, and the potential for fraud and identified risks were rated using a risk evaluation process that accounted for changes in risk the prior year, and were formally documented, along with the mitigation strategies, for management review.	No exceptions noted.
CC5.2.2	A documented risk assessment policy and program is in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the risk assessment policy to determine that a document risk assessment policy and program was in place that included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
CC5.2.3	Assigned risk owners select and develop control activities to mitigate the risks identified during the annual risk assessment process. The control activities are documented within risk treatment plans that are created by the risk owners for risks above the tolerable threshold.	Inspected the most recent risk assessment to determine that assigned risk owners selected and developed control activities to mitigate the risks identified during the period and the control activities were documented within risk treatment plans that were created by the risk owners for risks above the tolerable threshold.	No exceptions noted.
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	Job descriptions are documented for employees supporting the services and include authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system.	Inspected the documented job descriptions for a sample of employment positions to determine that job descriptions were documented for employees supporting the services and included authorities and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system for each position sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC5.3.2	Increase employees review and attest to their agreement with the information security policy that describes their responsibilities and expected behavior, including regarding data and information system usage on an annual basis.	Inspected the information security policy attestation for a sample of current employees to determine that each company employee sampled reviewed and attested to their agreement with the information technology security policy that described their responsibilities and expected behavior, including regarding data and information system usage during the period.	No exceptions noted.
CC5.3.3	Increase maintains established policies and procedures, which outline operating practices and business conduct for employees and contractors. Policies and procedures are reviewed periodically (but not less than annually) and updated when needed. The policies and procedures include the following: • Incident response plan • Information security policy • DR plan • Risk assessment policy	Inspected the policies and procedures to determine that Increase maintained established policies and procedure, which outlined operating practices and business conduct for employees and contractors and policies and procedures were reviewed and updated during the period for each of the following policies: • Incident response plan • Information security policy • DR plan • Risk assessment policy	No exceptions noted.
CC5.3.4	System users are given instructions with respect to access credential security in the company's documentation and in their service agreement with Increase.	Inspected the external company website and the standard customer contracts to determine that system users were given instructions with respect to access credential security in the company's documentation and in their service agreement with Increase.	No exceptions noted.
Logical and Physical Access Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Documented policies and procedures are in place to guide information security practices that include, but are not limited to, the following: • Account management • Password requirements • Protecting proprietary information	Inspected the information security policy to determine that document policies and procedures were in place to guide information security practices that included, but were not limited to, the following: • Account management • Password requirements • Protecting proprietary information	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.2	The in-scope systems are configured to authenticate users with unique user accounts and minimum password requirements or multi-factor authentication where possible.	Inspected the user account listing and authentication configurations for a sample of in-scope systems to determine that the following sampled in-scope systems were configured to authenticate users with unique user accounts and minimum password requirements or multi-factor authentication where possible: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.1.3	Predefined security groups are utilized to assign role-based access privileges and segregate access to data for the in-scope systems.	Inspected the user account listing and the administrator user account listing for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the following sampled in-scope systems: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.1.4	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listing for a sample of in-scope systems with the assistance of the head of engineering to determine that administrative access privileged to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.1.5	Google Cloud VPC firewall is configured to allow permitted access and deny unauthorized access.	Inspected the Google Cloud VPC firewall configurations to determine that the Google Cloud VPC firewall was configured to allow permitted access and deny unauthorized access.	No exceptions noted.
CC6.1.6	On an annual basis, the master asset listing is reviewed by management for completeness and accuracy.	Inspected the most recent master asset listing review to determine that the master asset listing was reviewed by management for completeness and accuracy during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.1.7	Company managed laptop disks are required to use full disk encryption.	Inspected the laptop encryption configurations for a sample of current employee's laptops to determine that each company managed laptop sampled used full disk encryption.	No exceptions noted.
	Google is responsible for ensuring data within GCP is stored in an encrypted at rest format.		
	Google is responsible for ensuring access to Cloud Storage server-side encryption keys is restricted to authorized personnel.		
	Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
CC6.2 Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	Administrators grant or modify access to Increase systems after approval by the hiring manager.	Inspected the listing of user accounts to in-scope systems with the assistance of the head of engineering and determined that there were no users that was provisioned access during the period; therefore, no testing of operating effectiveness was performed.	
CC6.2.2	Management notifies system administrators when employees are terminated. System administrators revoke user accounts assigned to terminated employees upon notification.	Inspected the termination request ticket for a sample of employees terminated during the period and the user account listings for in-scope systems to determine that management notified system administrators when employees were terminated, and system administrators revoked user accounts assigned to terminated employees upon notification for each employee and in-scope systems sampled: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.2.3	Increase reviews users access levels at least annually, including an independent review of the access levels of the individual conducting the review.	Inspected the most recently performed user access review documentation to determine that Increase reviewed user access levels, including an independent review of the access levels of the individual conducting the review, during the period.	No exceptions noted.
	Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
CC6.3 The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	Administrators grant or modify access to Increase systems after approval by the hiring manager.	Inspected a listing of users with access to in-scope systems with the assistance of the head of engineering and determined that there were users provisioned access during the period; therefore, no testing of operating effectiveness was performed.	

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.2	Management notifies system administrators when employees are terminated. System administrators revoke user accounts assigned to terminated employees upon notification.	Inspected the termination request ticket for a sample of employees terminated during the period and the user account listings for in-scope systems to determine that management notified system administrators when employees were terminated, and system administrators revoked user accounts assigned to terminated employees upon notification for each employee and in-scope systems sampled: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.3.3	Increase reviews users access levels at least annually, including an independent review of the access levels of the individual conducting the review.	Inspected the most recently performed user access review documentation to determine that Increase reviewed user access levels, including an independent review of the access levels of the individual conducting the review, during the period.	No exceptions noted.
CC6.3.4	The in-scope systems are configured to authenticate users with unique user accounts and minimum password requirements or multi-factor authentication where possible.	Inspected the user account listing and authentication configurations for a sample of in-scope systems to determine that the following sampled in-scope systems were configured to authenticate users with unique user accounts and minimum password requirements or multi-factor authentication where possible: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.3.5	Administrative access privileges to the in-scope systems are restricted to user accounts accessible by authorized personnel.	Inspected the administrator user account listing for a sample of in-scope systems with the assistance of the head of engineering to determine that administrative access privileged to the following sampled in-scope systems were restricted to user accounts accessible by authorized personnel: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.3.6	Predefined security groups are utilized to assign role-based access privileges and segregate access to data for the in-scope systems.	Inspected the user account listing and the administrator user account listing for a sample of in-scope systems to determine that predefined security groups were utilized to assign role-based access privileges and segregate access to data for the following sampled in-scope systems: • Google workspace • Google management console • Production databases • Production servers	No exceptions noted.
CC6.3.7	Increase maintains information security policies that address information security controls for accessing sensitive system environments.	Inspected the information security policy to determine that Increase maintained information security policies that addressed information security controls for accessing sensitive system environments.	No exceptions noted.
	Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
	Google is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
CC6.5 The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
	Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
	Google is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.		
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	Google Cloud VPC firewall is configured to allow permitted access and deny unauthorized access.	Inspected the Google Cloud VPC firewall configurations to determine that the Google Cloud VPC firewall was configured to allow permitted access and deny unauthorized access.	No exceptions noted.
CC6.6.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the web server encryption configurations to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.6.3	An IDS is used to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was used to analyze network events and report possible or actual network security breaches.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Google is responsible for implementing controls to manage logical access to the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
CC6.7 The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	An IDS is used to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was used to analyze network events and report possible or actual network security breaches.	No exceptions noted.
CC6.7.2	Web servers utilize TLS encryption for web communication sessions.	Inspected the web server encryption configurations to determine that web servers utilized TLS encryption for web communication sessions.	No exceptions noted.
CC6.7.3	Data and information critical to the system is mapped and assessed annually for relevance and use.	Inspected the most recent data and information review and the related documentation to determine that data and information critical to the system was mapped and assessed for relevance and use during the period.	No exceptions noted.
CC6.7.4	Formal procedures are documented that outline the process Increase's staff follows to backup and recover customer data.	Inspected the backup restoration procedures to determine that formal procedures were documented that outlined the process Increase's staff followed to backup and recover customer data.	No exceptions noted.
	Google is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the Increase systems reside.		
CC6.8 The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The ability to install applications or software is restricted to authorized engineering personnel.	Inspected the listing of user accounts with the ability to install applications or software with the assistance of the head of engineering to determine that the ability to install applications or software was restricted to authorized engineering personnel.	No exceptions noted.
CC6.8.2	An IDS is used to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was used to analyze network events and report possible or actual network security breaches.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC6.8.3	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC6.8.4	Company managed laptop disks are required to use full disk encryption.	Inspected the laptop encryption configurations for a sample of current employee's laptops to determine that each company managed laptop sampled used full disk encryption.	No exceptions noted.
System Operations			
CC7.1 To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Cloud configuration is managed in Terraform. Changes are tracked in the git repository. Terraform changes go through the engineering team's change management process.	Inspected the terraform configuration and change documentation for a sample of cloud configuration changes implemented during the period to determine that cloud configuration was managed in Terraform and that each change sampled was tracked in the git repository and went through the engineering team's change management process.	No exceptions noted.
CC7.1.2	Container image integrity is verified in the production environment before running.	Inspected the container image configurations for a sample of containers to determine that container image integrity was verified in the production environment before running for each container sampled.	No exceptions noted.
CC7.1.3	Security vulnerabilities that are detected are triaged by the engineering team and monitored through resolution.	Inspected the remediation tickets for a sample of security vulnerabilities during the period to determine that each vulnerability sampled that was detected was triaged by the engineering team and monitored through resolution.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.1.4	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan on the company intranet to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC7.1.5	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.
CC7.1.6	Google Cloud VPC firewall is configured to allow permitted access and deny unauthorized access.	Inspected the Google Cloud VPC firewall configurations to determine that the Google Cloud VPC firewall was configured to allow permitted access and deny unauthorized access.	No exceptions noted.
CC7.1.7	A log management and metrics management tool is utilized to identify trends that may have a potential impact on Increase's ability to achieve its security objectives.	Inspected the log management and metric management tool configurations to determine that a log management and metric management took was utilized to identify trends that may have a potential impact on Increase’s ability to achieve its security objectives.	No exceptions noted.
CC7.1.8	An IDS is used to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was used to analyze network events and report possible or actual network security breaches.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan on the company intranet to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC7.2.2	Increase's employee handbook contains a requirement for employees to maintain the security and confidentiality of system data.	Inspected the employee handbook to determine that Increase's employee handbook contained a requirement for employees to maintain the security and confidentiality of system data.	No exceptions noted.
CC7.2.3	An IDS is used to analyze network events and report possible or actual network security breaches.	Inspected the IDS configurations and an example alert generated during the period to determine that an IDS was used to analyze network events and report possible or actual network security breaches.	No exceptions noted.
CC7.2.4	Enterprise monitoring applications are in place to monitor the performance and availability of production servers and devices.	Inspected the monitoring applications configurations and example alerts generated during the period to determine that the following enterprise monitoring applications were in place to monitor the performance and availability of product servers and devices.	No exceptions noted.
CC7.2.5	Penetration testing for sensitive systems is performed on an annual basis by an independent third-party vendor. Third-party reports are obtained identifying the findings and resolutions. If applicable, a remediation plan is developed and changes are implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	Inspected the most recent penetration test results to determine that penetration testing for sensitive systems was performed during the period by an independent third-party vendor and that reports were obtained identifying the findings and resolutions, and if applicable, a remediation plan was developed and changes were implemented to remediate critical and high findings, at a minimum, identified during the penetration test.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.2.6	A log management and metrics management tool is utilized to identify trends that may have a potential impact on Increase's ability to achieve its security objectives.	Inspected the log management and metric management tool configurations to determine that a log management and metric management took was utilized to identify trends that may have a potential impact on Increase’s ability to achieve its security objectives.	No exceptions noted.
CC7.2.7	An annual report on security events is given to management.	Inspected the most recent report on security events and the recurring security incident meeting invite to determine that a report on security events was given to management during the period.	No exceptions noted.
CC7.2.8	Continuous control monitoring is performed to gain assurance that controls related to security are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the monitoring tools configurations and example alerts generated during the period to determine that continuous control monitoring was performed to gain assurance that controls related to security were in place and operated effectively.	No exceptions noted.
		Inspected the security incident ticket for a sample of security incidents during the period to determine that corrective actions were taken by management based on relevant findings and tracked to resolution for each incident sampled.	No exceptions noted.
	Google is responsible for monitoring the logical access control systems for the underlying network, virtualization management software, and storage devices for its cloud hosting services where the Increase systems reside.		
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan and compliance program dashboard to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC7.3.2	Continuous control monitoring is performed to gain assurance that controls related to security are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the monitoring tools configurations and example alerts generated during the period to determine that continuous control monitoring was performed to gain assurance that controls related to security were in place and operated effectively.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the security incident ticket for a sample of security incidents during the period to determine that corrective actions were taken by management based on relevant findings and tracked to resolution for each incident sampled.	No exceptions noted.
CC7.3.3	Reported or detected security incidents are tracked within an internal collaboration tool until resolved. Security incidents are reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved.	Inspected the internal collaboration tool configurations and the security incident ticket for a sample of security incidents during the period to determine that reported or detected security incidents were tracked within an internal collaboration tool until resolved and that security incidents were reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved, for each incident sampled.	No exceptions noted.
CC7.4 The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	A formal incident response plan is communicated to employees via the company intranet and provides the following information: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	Inspected the incident response plan on the company intranet to determine that a formal incident response plan was communicated to employees via the company intranet and provided information including: • Communication method for reporting security incidents • Incident handling procedures • Instructions for reporting security violations	No exceptions noted.
CC7.4.2	Continuous control monitoring is performed to gain assurance that controls related to security are in place and operating effectively. Corrective actions are taken by management based on relevant findings and tracked to resolution.	Inspected the monitoring tools configurations and example alerts generated during the period to determine that continuous control monitoring was performed to gain assurance that controls related to security were in place and operated effectively.	No exceptions noted.
		Inspected the security incident ticket for a sample of security incidents during the period to determine that corrective actions were taken by management based on relevant findings and tracked to resolution for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC7.4.3	Reported or detected security incidents are tracked within an internal collaboration tool until resolved. Security incidents are reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved.	Inspected the internal collaboration tool configurations and the security incident ticket for a sample of security incidents during the period to determine that reported or detected security incidents were tracked within an internal collaboration tool until resolved and that security incidents were reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved, for each incident sampled.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	Data backup restoration tests are performed at least annually to verify data reliability and information integrity.	Inspected the most recent backup restoration test to determine that data backup restoration tests were performed during the period to verify data reliability and information integrity.	No exceptions noted.
CC7.5.2	Formal procedures are documented that outline the process Increase's staff follows to backup and recover customer data.	Inspected the backup restoration procedures to determine that formal procedures were documented that outlined the process Increase’s staff followed to backup and recover customer data.	No exceptions noted.
CC7.5.3	A documented BC / DR plan is in place and tested annually.	Inspected the BC / DR plan and the most recent BC / DR plan test results to determine that a documented BC / DR plan was in place and tested during the period.	No exceptions noted.
CC7.5.4	Reported or detected security incidents are tracked within an internal collaboration tool until resolved. Security incidents are reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved.	Inspected the internal collaboration tool configurations and the security incident ticket for a sample of security incidents during the period to determine that reported or detected security incidents were tracked within an internal collaboration tool until resolved and that security incidents were reviewed by management to ensure that the incident response procedures were followed, and that the incident was resolved, for each incident sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
Change Management			
CC8.1 The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	Documented change management policies and procedures are in place to guide personnel in performing change activities.	Inspected the change management policy to determine that documented change management policies and procedures were in place to guide personnel in performing change activities.	No exceptions noted.
CC8.1.2	A change management ticketing system is used to log and track change information, including testing and approval.	Inspected the change documentation for a sample of application and infrastructure changes implemented during the period to determine that a change management ticketing system was used to log and track change information, including testing and approval for each change sampled.	No exceptions noted.
CC8.1.3	Application development personnel utilize version control software to manage application development and maintenance activities. Changes are capable of being rolled back to prior versions of the application code as needed.	Inspected the version control software configurations to determine that application development personnel utilized version control software to manage application development and maintenance activities, and that changes were capable of being rolled back to prior versions of the application code as needed.	No exceptions noted.
CC8.1.4	Write access to the version control software is restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with write access to the version control software with the assistance of the head of engineering to determine that write access to the version control software is restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.5	Administrative access privileges to the version control software are restricted to user accounts accessible by authorized personnel.	Inspected the listing of user accounts with administrative access privileges to the version control software with the assistance of the head of the engineering to determine that administrative access privileged to the version control software were restricted to user accounts accessible by authorized personnel.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.6	Access privileges to promote changes into the production environment are restricted to user accounts accessible by authorized personnel.	Inspected the listing of users with accounts to promote changes into the production environment with the assistance of the head of engineering to determine that access privileges to promote changes into the production environment were restricted to user accounts accessible by authorized personnel.	No exceptions noted.
CC8.1.7	Program development and testing efforts are performed in distinct development and QA environments that are logically separated from the production environment.	Inspected the production environment and QA environment configurations to determine that program development and testing efforts were performed in distinct development and QA environments that were logically separated from the production environment.	No exceptions noted.
CC8.1.8	There is a test suite that runs against the code to determine if the change meets the business objective.	Inspected the completed test suite documentation for a sample of application and infrastructure changes implemented during the period to determine that there was a test suite that ran against the code to determine if the change met the business objective for each change sampled.	No exceptions noted.
CC8.1.9	An automated patch management tool is in place to monitor for new patches to relevant systems.	Inspected the automated patch management tool configuration, a completed patch log, and an example alert generated during the period to determine that an automated patch management tool was in place to monitor for new patches to relevant systems.	No exceptions noted.
CC8.1.10	The automated deployment tool is configured to alert IT and engineering personnel via the internal team collaboration tool when deployments occur.	Inspected the automated deployment tool configuration and an example alert generated during the period to determine that the automated deployment tool was configured to alert IT and engineering personnel via the internal team collaboration tool when deployments occurred.	No exceptions noted.
CC8.1.11	Reviews of time-sensitive changes implemented to the production environment are performed on a bi-weekly basis to help ensure that only authorized changes were made to the system.	Inspected the change review documentation for a sample of weeks during the period to determine that reviews of time-sensitive changes implemented to the production environment were performed to ensure that only authorized changes were made to the system for each week sampled.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC8.1.12	The automated deployment tool is configured to alert users when the branch protection is disabled.	Inspected the automated deployment tool configurations and example alerts generated during the period to determine that the automated deployment tool was configured to alert users even when the branch protection configuration is disabled.	No exceptions noted.
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The entity has purchased insurance to offset the financial loss that could result from a critical security incident or exploitation of a vulnerability.	Inspected the liability certificate of insurance to determine that the entity had purchased insurance during the period to offset the financial loss that could have resulted from a critical security incident or exploitation of a vulnerability.	No exceptions noted.
CC9.1.2	Management develops risk mitigation strategies to address risks identified during the risk assessment process.	Inspected the risk assessment policy and the most recently completed risk assessment documentation to determine that management developed risk mitigation strategies to address risks identified during the risk assessment process.	No exceptions noted.
CC9.1.3	A multi-location strategy is employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	Inspected the production environment configuration to determine that a multi-location strategy was employed for production environments to permit the resumption of operations at other availability zones in the event of the loss of a facility.	No exceptions noted.
CC9.1.4	Critical databases are run in high-availability mode to replicate data to a second location to mitigate the impact of a single location being lost.	Inspected the replication configuration for a sample of in-scope critical databases to determine that each critical database sampled ran in high-availability mode to replicate data to a second location to mitigate the impact of a single location being lost.	No exceptions noted.
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	Management obtains and reviews SOC reports for subservice organizations on an annual basis.	Inspected the most recent SOC review documentation for a sample of subservice organizations to determine that management obtained and reviewed SOC reports for each organization sampled during the period.	No exceptions noted.

Control #	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
CC9.2.2	A vendor security and risk assessment is performed as part of a due diligence review when considering a new vendor.	Inspected the vendor security risk assessment for a sample of vendors onboarded during the period to determine that a vendor security and risk assessment was performed as part of a due diligence review for each vendor sampled.	No exceptions noted.
CC9.2.3	Identified third party risks are rated using a risk evaluation process and ratings are approved by management.	Inquired of the chief compliance officer to determine that identified third party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
		Inspected the risk assessment policy and the most recently completed risk assessment documentation to determine that identified third party risks were rated using a risk evaluation process and ratings were approved by management.	No exceptions noted.
CC9.2.4	Management has defined roles and responsibilities to oversee the management of risks associated with vendors and business partners.	Inspected the audit and compliance committee charter to determine that management had defined roles and responsibilities to oversee the management of risks associated with vendors and business partners.	No exceptions noted.