Heap, Inc.

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, Processing Integrity, and Confidentiality Throughout the Period March 1, 2022, to March 31, 2023.

KirkpatrickPrice

4235 Hillsboro Pike
Suite 300
Nashville, TN 37215

TABLE OF CONTENTS

SECTION I:
ASSERTION OF HEAP MANAGEMENT

ASSERTION OF HEAP MANAGEMENT

We have prepared the accompanying description in section III titled "Heap's Description of Its Software-as-a-service System" throughout the period March 1, 2022, to March 31, 2023, (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 software-as-a-service system that may be useful when assessing the risks arising from interactions with Heap's system, particularly information about system controls that Heap 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, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Heap uses the following subservice organizations:

- Amazon Web Services (AWS) for cloud hosting
- Datadog for logging and monitoring the production environment
- Logz.io for logging for the legacy production environment
- PagerDuty for production environment event and incident alerting

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

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

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

a. the description presents Heap's software-as-a-service system that was designed and implemented throughout the period March 1, 2022, to March 31, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period March 1, 2022, to March 31, 2023, to provide reasonable assurance that Heap'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 and user entities applied the complementary controls assumed in the design of Heap's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period March 1, 2022, to March 31, 2023, to provide reasonable assurance that Heap's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Heap's controls operated effectively throughout that period.

SECTION II:
INDEPENDENT SERVICE AUDITOR'S REPORT

Ken Fine
Chief Executive Officer
Heap, Inc.
225 Bush Street, Suite 200
San Francisco, CA 94104

Scope

We have examined Heap's accompanying description in section III titled "Heap's Description of Its Software-As-A-Service System" throughout the period March 1, 2022, to March 31, 2023, (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 March 1, 2022, to March 31, 2023, to provide reasonable assurance that Heap's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, confidentiality, and processing integrity (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Heap uses the following subservice organizations:

- Amazon Web Services (AWS) for cloud hosting
- Datadog for logging and monitoring the production environment
- Logz.io for logging for the legacy production environment
- PagerDuty for production environment event and incident alerting

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Heap, to achieve Heap's service commitments and system requirements based on the applicable trust services criteria. The description presents Heap's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Heap's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Heap 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 Heap's service commitments and system requirements were achieved. In section I, Heap has provided its assertion titled "Assertion of Heap Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Heap is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the

description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description

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

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

Inherent Limitations

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 or 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 policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents Heap's software-as-a-service system that was designed and implemented throughout the period March 1, 2022, to March 31, 2023, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period March 1, 2022, to March 31, 2023, to provide reasonable assurance that Heap'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 and user entities applied the complementary controls assumed in the design of Heap's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period March 1, 2022, to March 31, 2023, to provide reasonable assurance that Heap's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Heap's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of Heap, user entities of Heap's software-as-a-service system during some or all of the period March 1, 2022, to March 31, 2023, business partners of Heap subject to risks arising from interactions with the software-as-a-service 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 user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- 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
- 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.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

April 25, 2023

SECTION III:
HEAP'S DESCRIPTION OF ITS SOFTWARE-AS-A-SERVICE SYSTEM

Founded in 2013, Heap provides an analytics platform to its clients that allows them to capture data about how their customers use their products. The Heap platform is designed to allow the organization's clients to understand how people interact with their product, increase acquisition and retention, reduce engineering burden, and create a powerful product experience. With the Heap platform, the organization's clients are able to map out their product and establish meaningful key performance indicators (KPIs) at all levels. The KPIs can be used to measure the impacts of decisions, isolate problem areas, prioritize efforts, and tie granular activities to high-level business metrics.

Client Engagement and Platform Functionality

Typically, paying clients are initially taken through a guided onboarding exercise. During onboarding, clients receive training for effective use of the Heap analytics product to fully exploit its retroactive analysis capabilities enabled through automatic capture of user behavioral data. Onboarding typically also includes assistance in the initial setup of the account, permissions, and definitions.

Clients access the front end of Heap's software-as-a-service (SaaS) via the organization's website and mobile application. Clients can view event data, define events, and perform analysis. The product can integrate with the client's webpages, android applications, and iOS apps. Event listeners integrate with the clients application to ingest event data and send to Heap for processing. Event data is correlated with a user identity and stored in a PostgreSQL database cluster.

When onboarding new clients, the Marketing and Sales Development teams work to qualify leads and then hand the leads off to a Sales Representative. The Sales team makes an initial discovery call and, if the client wishes to proceed, the team hands them off to a Solutions Consultant. The Solutions Consultant then demonstrates the product, performs a technical validation, and sets up a proof-of-value installation of the product. This can be installed in the client's web or mobile application, or it can be set up with test data. If the installation takes place in the client's application, the steps used are similar to the normal onboarding process. Each step in the process is documented in Salesforce.

Clients negotiate with legal and finance and then sign a contract. The record in Salesforce is updated, which triggers a message in Slack to notify the Technical team, which begins onboarding. The Solutions Consultant has a hand-off call with the Technical team to initiate the onboarding process.

The organization's SaaS platform has a free trial feature, which is also used to onboard paying clients. The client self-enrolls, creates an account, and receives a welcome email with links to provide a guided experience on how to install. This process creates an account number that is associated with the client. If the client is using a web page, they follow instructions to add a JavaScript to their page. If using mobile applications, there are different software development kits (SDKs).

Auto-capture functionality is enabled on websites by placing a standard tracking script in the header, and for mobile applications, specific build-steps are integrated to compile in the auto-tracking code.

After data capture has started, the Event Visualizer can be used to interactively define relevant virtual events based on interactions with elements of the site/application. Virtual events can retroactively incorporate all user interactions back to the data retention limit or when the auto-capture was installed, whichever is the more recent. Heap offers the ability to export data to client's data warehouses. If the client requests the ability to export, then their data is copied to S3 hourly where they can access via a cross account role in AWS to pull data to their warehouse. Supported warehouses include BigQ, Redshift, Snowflake, and S3.

The user interface to the Heap software provides capabilities to perform graphing and funnel analysis over aggregate behavioral data. Graphs can also be collected in dashboards to monitor related relevant metrics in a single screen, and Heap allows for live outbound data warehouse synchronization where behavioral data can be further analyzed with dedicated BI tools.

Security commitments are dependent upon the client's needs. Heap proactively shares SOC 2 and Health Insurance Portability and Accountability Act (HIPAA) audits, and for most companies, this is sufficient. For mid-market companies, the organization requires completion of a security review and questionnaire. Enterprise-level customers often have more in-depth reviews and audits.

Locations

The San Francisco, CA and New York, NY locations are in scope for this audit.

Contractual Commitments

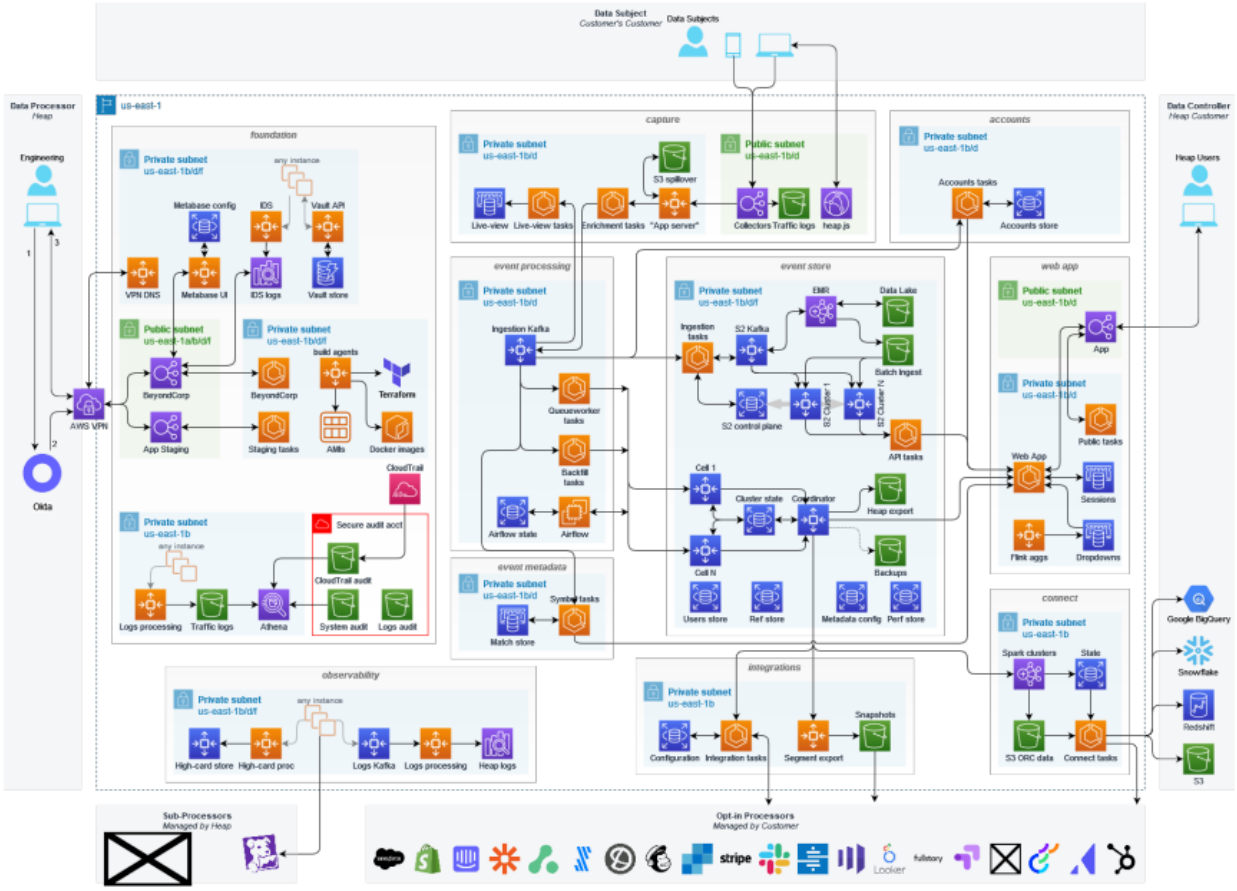
Heap executes contracts with its clients that describe the scope of services offered. Contracts vary depending on the size of the company, but all contracts link directly to Heap's website, which includes Heap's Terms of Service. Standard contracts do not include service-level agreements (SLAs). However, a pre-defined set of SLAs can be added upon request for certain categories of clients. Heap's service availability to customers is 99.5% of all scheduled availability, which is calculated annually. The organization also uses marketing materials published on its website to communicate the services it offers. The organization designs its security programs and business operations to maintain compliance with industry expectations and regulatory commitments.

System Design

Heap designs its SaaS system to meet its regulatory and contractual commitments. These commitments are based on the services that Heap provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Heap has established for its services. Heap establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Heap's system policies and procedures, system design documentation, and contracts with clients.

Infrastructure

The organization documents its network design for the purpose of showing its network inter-connectivity between its locations and the associated segmentation of various parts of network and perimeter security of its network via firewalls. To outline the topology of its network, the organization maintains the network diagram below to illustrate its internal infrastructure. The engineers are responsible for maintaining the network diagram for the AWS environment.



In addition, the organization maintains an inventory of production systems in AWS via the AWS console. Workstation inventory is maintained via Jamf.

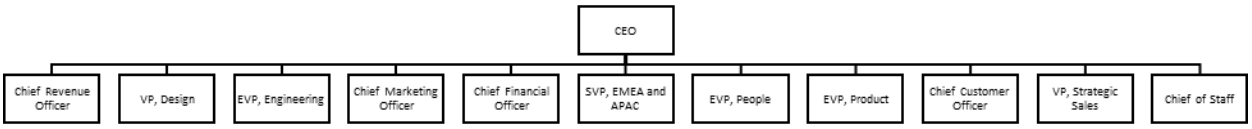
Software

The organization maintains an inventory of software in AWS via the AWS console. All other critical software is tracked manually. The following software is used in the development of Heap's SaaS platform:

- AWS
- Datadog
- Foxpass
- HelloSign
- PagerDuty
- Salesforce
- SendGrid
- Slack
- Statuspage
- Wazuh
- Zoom

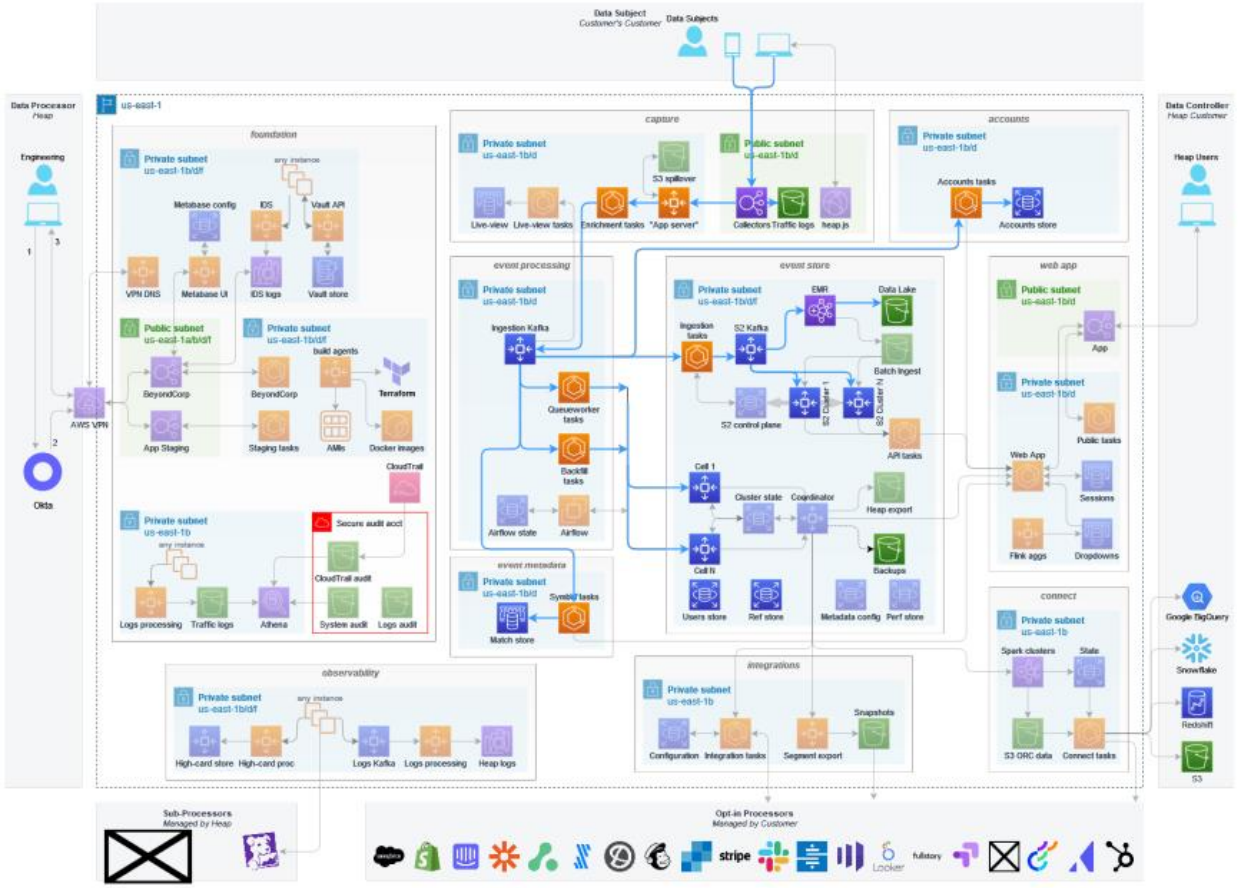
People

Heap has a traditional hierarchical structure with the CEO at the head of the organization. The organization is divided into seven departments led by department heads that report to the CEO. Security and Compliance personnel have a direct reporting line to management to maintain independence. The organization also has a seven-member board of directors that is comprised of the two co-founders and five independent parties. The main function of the board is to provide oversight regarding financial health and strategic direction for Heap. To outline its hierarchical structure, Heap maintains an organization chart, which has been summarized below to show the CEO and direct reports.



Data

To provide its services, the organization stores, processes, and transmits customer data as well as Heap business data and source code data. Data captured in Heap's system is intrinsically designed to be robust. The public capture application programming interface (API) by design must capture any and all traffic that hits it. Once data is captured, it is immediately stored in a fully redundant cluster for downstream processing. Access to captured data for a given customer is tied internally to a unique "app id" tied to the user login via the customer account. The system pervasively ensures that a given session can only ever access data captured and associated with the correct "app id" as a baseline data safety measure to avoid misrouting. The requests Heap handles from its customers involve requesting aggregate analytics over the captured end-user interactions within their sites and are intrinsically not susceptible to malicious subversion by any of the mentioned means. The organization maintains a data flow diagram to illustrate this flow of sensitive data throughout the environment. The Bedrock Engineering team is responsible for maintaining the diagram for the AWS environment.



In addition, the organization documents requirements for the handling of sensitive customer information. Detection algorithms are in place to detect and purge sensitive data that is collected incidentally. All confidential information transmitted via the internet is encrypted in transit using Transport Layer Security (TLS) 1.2 or higher by all systems. Heap uses the following technologies to assist in securing all transmissions over the internet:

- AWS Key Management System (KMS) for secret management within production

- AWS Certificate Manager for public TLS certificates
- Public internet-facing load balancers configured according to AWS best practices

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization's services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

The security, availability, confidentiality, and processing integrity categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security, availability, confidentiality, and processing integrity criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security, availability, confidentiality, and processing integrity criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of Heap's description of its SaaS system.

Control Environment

Management Philosophy

Management communicates the tone and direction of the organization through policy documents, employee training, meetings, and regular daily communication. Employees are required to acknowledge the Employee Handbook and participate in security awareness training. All policies are made available to employees electronically. Management hosts monthly all-hands meetings to discuss the organization's performance goals, and Slack is used to inform all personnel of company activities and meetings. Management uses policy documentation to communicate employee conduct expectations as well as the organization's commitment to integrity and ethics.

The organization develops a set of priorities for the fiscal year based on input from the leadership team. These are reviewed in an all-hands meeting and the Executive team reviews the progress toward those priorities weekly. Metrics are established and pushed down to the individual and departmental level to track progress toward the organization's priorities. A Slack channel is employed as a method for management to provide regular communication. Additionally, the organization has defined values. Performance reviews are performed every quarter to review employee performance relative to organizational priorities and values.

Regarding conduct, the organization requires all employees to sign and acknowledge the Heap Company Policy Handbook, which defines Heap's values and its Code of Conduct. The handbook is made available for all employees via BambooHR.

Security, Availability, Confidentiality, and Processing Integrity Management

The organization's security, availability, confidentiality, and processing integrity requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security, Availability, Confidentiality, and Processing Integrity Policies

Heap documents policy creation, modification, and review requirements in the Documentation Policies, the Policy Policies, and the Policy Review and Update Procedures. All major Heap policies are processed through a change management system, contain approvals, revision history, and current dates. The following policies documentation was reviewed during the audit period:

- Business Continuity & Capacity Policies
- Confidential Information Policies
- Data Destruction Policies
- Documentation Policies
- Employee Handbook: Guidebook & Policies
- Human Resources Policies
- Incident Management Policies
- Logical Security Policies
- Physical Security Policies
- Policy Policies
- Risk Management Policies
- System Development Policies
- System Operation Policies
- Third-Party Management Policies

Personnel Security

Heap maintains policies that describe requirements for hiring, termination, and other employee-related guidelines. The organization uses a standard set of forms, documents, and acknowledgements during the new-hire and termination process. To facilitate the hiring and termination procedures, the organization uses the onboarding checklist and the offboarding checklist. The organization also issues a Heap offer letter that includes a background check clause as well as a mutual arbitration agreement and a California Confidential Information and Invention Assignment Agreement (CIIAA) during the new-hire process.

During onboarding, the organization performs background checks on all new employees. Items covered during background checks include name, address, and date of birth verification; Social Security number (SSN) verification; and federal or state criminal record checks.

To ensure that employees are aware of their responsibilities, the organization has implemented the following:

- Employee Handbook—the handbook addresses code of business ethics and standards of conduct, acceptable use, and confidentiality
- Job Descriptions—the organization has job descriptions for all critical positions
- Employee Training—the organization requires all employees to participate in security awareness training upon hire and annually thereafter; HIPAA training is provided upon hire and every two years thereafter

All new hires receive the handbook as part of onboarding and must acknowledge their understanding of the included policies. The handbook is maintained in a location that is accessible by all personnel.

The organization has defined onboarding and offboarding checklists maintained in BambooHR. Onboarding activities include soliciting employee handbook acknowledgements, performing security and HIPAA awareness training, and conducting background checks. Background checks are conducted in accordance with local laws and regulations. Job candidates must successfully complete criminal background checks prior to being hired, and checks include the following verifications:

- Name
- Address
- Date of birth
- Official identification or SSN verification
- Federal and state criminal record check

Physical Security and Environmental Controls

Heap documents requirements for physical security controls implemented in its San Francisco and New York offices. Within both office facilities, the organization implements a badge access system, cameras, and visitor logs. The organization has a visitor registration process in place via an Envoy system.

In addition, the San Francisco and New York offices both exist within multi-tenant buildings whose building management teams oversee the alarm system for the buildings as a whole. The organization's production environment and data center, including all backups, are located entirely within the AWS environment. The physical and environmental security of all Heap assets housed within the AWS environment are the responsibility of AWS. The organization has collected and reviewed the latest AWS SOC2 Type II report to evaluate AWS's internal controls as they relate to the services provided to Heap.

Regarding backups and media disposal, all backups are performed and stored in the AWS cloud hosting environment. Employee laptops are stored securely onsite in the IT closets in the San Francisco or New York office until they can be wiped and destroyed or repurposed. The IT closets in both locations are locked with a physical key and only IT and the Office Manager have access to the key. The organization requires that laptops be wiped prior to reuse or disposal.

Additionally, the facilities are equipped with environmental safeguards that protect the company assets and monitor for fire, water, and intrusion-related incidents. Environmental controls such as fire alarms and fire extinguishers are in place that are managed by the buildings' management. Heap's most important defense against environmental hazards and disasters is its fundamentally decentralized nature. If the physical office were lost, it would not impact ongoing operation in a substantial way. The entire system is hosted in AWS cloud services. Sales staff use online communications and mobile devices to contact customers. Support is entirely mediated over the internet. In case of a disaster, all personnel could work remotely until the situation was resolved.

Configuration and Change Management

Heap has formal policies and documentation related to configuration and change management. Configuration requirements are outlined in the Security Guidelines for New Infrastructure, and the organization references the National Institute of Standards and Technology (NIST) and Center for Internet Security (CIS) hardening standards when developing configuration standards. Personnel responsible for configurations subscribe to industry-accepted practices/standards from organizations such as NIST, SANS, Open Worldwide Application Security Project (OWASP), and CIS. Engineering managers are responsible for ensuring that best practices are applied.

The Bedrock Engineering Team at Heap manages perimeter security. The organization employs AWS best practices and CIS benchmarks to firewall their AWS production environment, and the

San Francisco administrative office is protected with a firewall. Organizational policy requires that all workstations be configured with firewall enabled.

In the event that changes must be implemented in the Heap environment, the organization follows a formal change management policy. To track the change management process, the organization uses the Jira ticketing system. The change management process is executed with the following:

- Clearly identified roles and responsibilities
- Impact or risk analysis of the change request
- Testing prior to the implementation of change
- Authorization and approval
- Process for notifying clients prior to changes being made, which may impact their service
- Post-installation validation
- Backout or recovery plans

Regarding the change management process, the organization uses infrastructure as code (IaC) and manages production systems through pre-configured Terraform modules. Base advanced metering infrastructures (AMIs) for all servers are the same and incorporate NIST and CIS standards. Ephemeral servers are destroyed and rebuilt every time that code is released, which happens weekly. Each time a system is rebuilt it is built with the most recent version of the OS. The following attributes are configured using bash scripts associated with the AMIs:

- OS hardening
- Vault certificates
- Network Time Protocol (NTP)
- An intrusion detection system (IDS) and logging agents

In addition, the organization uses AWS security groups and virtual private clouds (VPCs) to control internet traffic to and from its systems.

Application Development

The System Development Policies document describes the software development lifecycle. Heap ensures security of the development process by executing the policies included in the System Development Policies, including the separation of the development, test, and production environments. Development is performed on local computers, during which engineers check out code and then issue a pull request (PR) for code to be reviewed by another team member. The testing environment is housed physically and logically separated from the development and production environments. The duties of development, test, and production personnel are outlined in the System Development Policies and in the detailed engineering organization chart.

To further secure the development process, the organization restricts access to source code and implements version controls and executes code review and testing. Access to the GitHub source code repository is granted based on principles of least privilege, and version control is applied through automated tools in GitHub. The organization ensures applications are not susceptible to vulnerabilities by executing code reviews and performing vulnerability scans and web application penetration testing.

In addition, code repositories are maintained in GitHub, and access is strictly controlled. The organization adheres to the principle of least privilege where the minimum rights and privileges necessary are assigned to a user based on the user's job requirements. Access to GitHub requires multi-factor authentication (MFA), and administrator access to repositories are reviewed at least quarterly.

Developers develop code on local machines and test locally with anonymized data when necessary. All code changes require peer review before they are approved to merge to production. Part of the process of code review includes checking for OWASP Top 10 vulnerabilities. Build kit orchestrates code deployment on Heap assets within the asset's own VPC. Results are then published to Amazon S3, where they can be deployed to all systems. Various tools for static analysis are incorporated into the development process, including the following:

- Danger
- ESLint
- Checkov
- Proto Lint
- ShellCheck
- Secret Linter

Application Change Management

Heap implements application changes according to the Change Management Policy. The code repository in GitHub is integrated with the Jira ticketing system in which tickets are created to document and track application changes. Approved and tested changes are pushed to production continuously with backout procedures in place for every change committed. The organization has a process for notifying clients prior to changes that may impact their service. As part of the application change management process, the organization establishes the following requirements and procedures:

- Technical specifications are developed for significant changes and documented in Jira
- Source code is checked-out and developed on local machines
- Code review is required
- Program changes are tested in a separate, controlled environment
- Code deployment is automated via Buildkite
- Backout can be performed using a reverse PR in GitHub, if necessary

System Monitoring

The organization has established multiple means of monitoring the security, availability, confidentiality, and processing integrity of its systems. Heap has formal logging and monitoring policies and procedures documented in the System Development Policies document and the System Operation Policies document. The organization uses AWS CloudTrail to monitor the AWS environment. AWS CloudTrail is enabled in all regions, and AWS CloudTrail log file validation is enabled. Datadog is used to monitor system capacity and related metrics. Security-related logs for AWS CloudTrail are stored in S3 buckets and encrypted using AES-256. Application logs are stored in Logz.io. Logs contain at least the following information:

- Source IP
- Destination IP
- Destination port
- Protocol type
- Timestamp

The Incident Management Policies and the System Operation Policies documents describe how the organization is required to monitor alerts from intrusion detection and prevention systems (IDS/IPS), alerts from file-integrity monitoring systems (FIM), and detection of unauthorized wireless access points. The organization uses Wazuh to monitor network traffic for suspicious activity. PagerDuty and Slack are used to notify responsible employees when anomalies are detected.

Datadog is used to monitor the health of Heap's AWS environment. Heap uses Wazuh for IPS, FIM, and rootkit protection on all production servers. Wazuh monitors for configuration changes, rootkits, attempted exploits, and bursts of authentication failures. Wazuh integrates with PagerDuty to notify the appropriate personnel when anomalies are detected.

The organization performs regular scanning, including an annual penetration test, and weekly scans using AWS native tools, such as Trusted Advisor. In addition, the organization requires event logging. The following types of logs are used by the organization:

- Security-related logs for CloudTrail, which are stored in a read-only state in S3
- Application logs in S3 buckets, which are stored for a rolling 14-day period
- Legacy application logs in Logz.io, which are archived for a rolling 14-day period
- Application logs in Wazuh, which are archived for a rolling 14-day period

The organization requires all systems to be protected from unauthorized or malicious software. Workstations have the Jamf antivirus solution installed, and an Wazuh agent is installed on production servers.

Regarding patching, employee laptops are patched automatically via Jamf. The AWS production environment is maintained via Terraform. Heap uses IaC to tear down and deploy infrastructure weekly. Servers are built from a golden AMI that is updated monthly with the newest security patches and any necessary configuration changes.

Problem Management

Heap has developed and implemented a formal incident response process for identifying, reporting, containing, and eradicating incidents and breaches. All engineers participate in the incident response process as part of an on-call rotation. Production alerts trigger PagerDuty and Slack channel and have a Playbook for triage of the alert. If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist. Data breaches require specific steps as detailed in the incident management policies. The incident management policies define the following:

- What specific events are considered a security incident
- Workforce members' role and responsibilities regarding security incidents
- Management involvement regarding security incidents
- What steps should be taken in response to a security incident
- Annual testing of the incident response procedures if they are not triggered organically

In addition, new engineers shadow experienced engineers to receive training related to incident response procedures before they are placed on the on-call rotation. Real security events are

analyzed and lessons learned are used to perform training for all employees with incident management responsibilities.

The organization provides communication channels for customers and personnel to report suspected breaches or security incidents. A dedicated email is used to contact the organization about suspected security incidents, and the organization's website displays contact information for Heap.

Data Backup and Recovery

Heap has formally documented backup and business continuity policies and procedures. The organization executes daily snapshot backup jobs, and the organization completes data restoration jobs. All backups occur entirely within the AWS environment and are encrypted.

Regarding backups, the organization requires that encrypted backups be implemented for all customers. Backups are being performed as follows:

- Amazon Relational Database Service (RDS) is performed nightly for all databases and is retained for six days
- Customer data, Elasticsearch, and GitHub are copied out to Amazon S3 nightly and retained for at least three months

A recovery time objective (RTO) of 24 hours is defined by the organization. A recovery point objective (RPO) of five minutes is established for critical business processes.

The organization has a Business Continuity & Capacity Policies document that describes the plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following an interruption to, or failure of, critical business processes. Policies require the organization to test its business continuity plans at least annually.

The business continuity plans are updated and tested annually to assess the current state of the organization and its ability to restore operations in any given scenario. To test the plan, the organization conducts a tabletop exercise and documents all lessons learned within the test and corresponding remediation plans.

System Account Management

Logical access controls are documented within the Logical Security Policies. The organization uses various logical access control systems, including Okta and AWS System Session Manager, to enforce logical access restrictions. Before logical access is granted to new employee users, access is formally requested through Jira. Once user access has been approved, users are assigned unique IDs that are provisioned with least-privilege access. Users have only the access that their specific job responsibilities require. The organization enforces MFA for all users via Okta, and requires MFA be enabled for remote access to systems. Additionally, the organization uses Foxpass to authenticate Secure Shell (SSH) access to production systems.

In the event that employees are terminated, the organization immediately revokes access from the terminated user and records the same in an offboarding checklist. When employees are terminated, Heap creates a copy of an offboarding checklist template that is used to track all

tasks related to offboarding. The highest priority item includes removing access for critical systems.

Heap secures employee accounts by enforcing account security measures, including password parameters. The following is in place to protect employee user accounts for accessing the AWS environment:

- Password complexity requires the use of uppercase and lowercase characters, a symbol, and a number
- Minimum password length is set to eight
- Maximum password age is 180 days

The organization securely stores passwords and if they must be transmitted they are done so using at least TLS 1.2 encryption. In addition to password requirements, the organization enforces the use of a virtual private network (VPN) with MFA for remote access.

The organization also has formal procedures for registering and deregistering client users; this process is detailed in the Customer Implementation Guide. Users of the Heap application are added when the customer's account is set up and the customer administrator may add or delete users for their particular account at any time.

Risk Assessment Process

Heap has a formal, documented Risk Management Policy that documents requirements for reviewing risk assessments quarterly. The risk assessment process is in place to identify the organization's critical assets that require protection and to understand and document risks from security failures that may cause loss of confidentiality, integrity, or availability. The organization has a process in place for all employees to identify and submit risks via templated Jira tickets. Quarterly, managers review the existing risk register and any newly identified risks, and mitigation plans are tracked via Jira with the highest severity risks being prioritized. The risk assessment provides guidance for the analysis of risks and how they should be handled and is used to determine the appropriateness of selecting controls that transfer, avoid, and mitigate risk.

Information and Communication Systems

Information security is covered by multiple Heap policies, and the organization's information security policies define information security responsibilities for all personnel. The organization reviews information security policies at least annually and the policies are made available to all employees electronically via Confluence.

The organization maintains best practices documents for using its products and services. Clients are made aware of the documentation portal and diverse documentation there.

The organization also has a formal privacy policy, which addresses privacy practices at Heap. The policy is made available for all users via the organization's website.

Vendor Management

Heap has a Third-Party Management Policies document in place that describes the organization's process for engaging with vendors. The policy specifies that the organization uses a Third-Party Solution Assessment template to conduct due diligence on new third parties, and the assessment process is initiated from the Slack channel for #vendor-review. Due diligence for service providers gets documented in a company third-party Solution Registry. The organization evaluates the service delivery and compliance status of its service providers by collecting applicable audit reports and completing third-party solution assessments. NDAs are executed with third parties to ensure any sensitive data is protected.

Monitoring Controls

Heap performs monitoring activities to ensure operational quality and control. The organization monitors website and application availability and responsiveness as well as data processing latency, backup run completion, timely completion of critical tasks, exports, and synchronizations. Disk usage, web host health in the load balancer, latency spikes, and CPU spikes (by Datadog) are also monitored. The organization documents guidelines for operational and security procedures and monitors its production environment for performance and availability using a variety of tools, including Datadog and Wazuh. The tools generate alerts via integration with PagerDuty, which are monitored constantly by the Engineering team to ensure quality delivery of the application.

In addition, management keeps a risk register that is actively populated and reviewed at least quarterly. Independent security and penetration testing are conducted at least annually. The organization undergoes a SOC 2 audit annually and a HIPAA audit, which is performed every other year. Management reviews the list of exceptions and recommendations from the audit and creates remediation plans, which are documented in Jira.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the SaaS system during the period from March 1, 2022, through March 31, 2023.

COMPLEMENTARY USER-ENTITY CONTROLS

Heap's services are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Heap's management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Heap also provides best practice guidance to clients regarding control element outside the sphere of Heap responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Heap controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Heap.

- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Heap's services.

- Transactions for user organizations relating to Heap's services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to Heap, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Heap's services.

- User organizations should report to Heap in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Heap.

- User organizations are responsible for notifying Heap in a timely manner of any changes to personnel directly involved with services performed by Heap. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Heap.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Heap.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Heap.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

SECTION IV:
TRUST SERVICES CATEGORIES, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

APPLICABLE TRUST SERVICES CRITERIA RELEVANT TO SECURITY, AVAILABILITY, CONFIDENTIALITY, AND PROCESSING INTEGRITY

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of Heap's (Heap's) system description throughout the period March 1, 2022, to March 31, 2023.

Security

The trust services criteria relevant to security address the need for information and systems to be protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the service organization's ability to achieve its service commitments and system requirements.

Security refers to the protection of

i. information during its collection or creation, use processing, transmission, and storage and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Heap's service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by Heap's systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Processing Integrity

The trust services criteria relevant to processing integrity address the need for system processing to be complete, valid, accurate, timely, and authorized to achieve the service organization's service commitments and system requirements.

Processing integrity refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether systems achieve the aim or purpose for

which they exist and whether they perform their intended functions in an unimpaired manner, free from error, delay, omission, and unauthorized or inadvertent manipulation.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements.

Confidentiality addresses Heap's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from Heap's control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Control Environment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	Heap communicates employee conduct expectations as well as its commitment to integrity and ethics through company policies.	Reviewed the Employee Handbook (dated March 2023) and verified that the organization maintains an employee handbook that contains the following: • Code of Conduct • Expectations for the compliance with legal regulations • Confidentiality requirements Interviewed the Executive Vice President (EVP) of People and the Senior Director of People Operations and determined that the Employee Handbook is distributed to each employee via the BambooHR platform; employees can access the handbook at any time from the platform Interviewed the Chief Financial Officer (CFO) and the EVP of Product and determined that the organization maintains value statements, such as Ownership, Respectful Candor, and having a Growth Mindset all of which have implications related to security and compliance Observed the website and verified that the organization documents value statements that are accessible on the site	No Relevant Exceptions Noted
CC1.1.2	Heap facilitates hiring and termination procedures through checklists.	Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization uses an onboarding checklist to hire and onboard new employees Observed employee records for a sample of 12 of 123 new hires and verified that an onboarding checklist	No Relevant Exceptions Noted

		was completed for all sampled employees Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization has the following processes in place for voluntary and involuntary terminations: • For voluntary terminations, HR is notified of the last date of employment and a ticket is submitted • For involuntary terminations, HR coordinates with IT to have the employee's account access revoked immediately upon notice of termination • BambooHR integrates with the IT ticketing system and creates a termination request Observed tickets for a sample of 14 of 144 terminated employees and verified that and verified that a termination ticket was submitted for all sampled former employees	
CC1.1.3	Heap uses a standard set of forms, documents, and acknowledgements during the new-hire and termination process.	Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization uses an onboarding checklist to hire and onboard new employees Observed employee records for a sample of 12 of 123 new hires and verified that an onboarding checklist was completed for all sampled employees Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees signed a non-disclosure agreement (NDA) and a noncompete clause Observed acknowledgements for a sample of 12 of 123 new hires and verified that all sampled employees acknowledged the Employee Handbook	No Relevant Exceptions Noted

		Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that employees are required to acknowledge an acceptable use policy and information security policies upon hire Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees acknowledge the information security policies Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization has the following processes in place for voluntary and involuntary terminations: • For voluntary terminations, HR is notified of the last date of employment, and a ticket is submitted • For involuntary terminations, HR coordinates with IT to have the employee's account access revoked immediately upon notice of termination • BambooHR integrates with the IT ticketing system and creates a termination request Observed tickets for a sample of 14 of 144 terminated employees and verified that and verified that a termination ticket was submitted for all sampled former employees	
CC1.1.4	Heap requires all employees to acknowledge the Employee Handbook, which addresses employee conduct requirements, both during onboarding and annually thereafter.	Interviewed the EVP of People and the Senior Director of People Operations and determined that the Employee Handbook must be acknowledged during the onboarding process by all employees Observed acknowledgements for a sample of 12 of 123 new hires and verified that all sampled employees acknowledged the Employee Handbook	No Relevant Exceptions Noted

CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	Heap has a traditional hierarchical structure that is headed by a CEO and has defined reporting lines.	Interviewed the CFO and the EVP of Product and determined that the organization is structured in a traditional hierarchy with departments organized according to responsibility and function Observed the organizational chart and verified that the organization is structured as a traditional hierarchy with the C-suite and EVPs reporting up to the CEO, and that the security and compliance personnel have a direct reporting to management to maintain independence	No Relevant Exceptions Noted
CC1.2.2	Heap has a board of directors that provides oversight to the organization.	Interviewed the CFO and the EVP of Product and determined that governance and oversight are provided by the board of directors, which meets quarterly Observed example board meeting minutes from a recent board meeting and verified that the board meets at least quarterly	No Relevant Exceptions Noted
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	Heap maintains organization charts that reflect the structure and reporting lines of the organization.	Interviewed the CFO and the EVP of Product and determined that the organization is structured in a traditional hierarchy with departments organized according to responsibility and function Observed the organizational chart and verified that the organization is structured as a traditional hierarchy with C-suite and EVPs reporting up to the CEO, and that the security and compliance personnel have a direct reporting to management to maintain independence	No Relevant Exceptions Noted
CC1.3.2	Heap maintains information security policies that describe responsibilities for all employees.	Reviewed the following documents and verified that the organization maintains information security policies to support internal controls and	No Relevant Exceptions Noted

		business objectives, and policies communicate the information security responsibilities of employees: • Human Resources Policies • Policy Policies • Physical Security Policies • Logical Security Policies • Confidential Information Policies • System Operation Policies • Risk Management Policies • Third-Party Management Policies • Incident Management Policies • Business Continuity & Capacity Policies • Communication Policies • System Development Policies • Documentation Policies • Data Destruction Policies Interviewed the Compliance Manager and determined that information security policies are reviewed annually Observed policy review tickets in Jira and verified that the organization's information security policies are reviewed annually Interviewed the CFO and the EVP of Product and determined the following: • The management team meets weekly • Departments meet at least weekly; in some cases, daily stand ups are held • Monthly all-hands meetings are held Observed the Outlook calendar of the CFO and the EVP of Product and verified that various meetings are held with varying cadences	
CC1.3.3	Heap uses job descriptions to communicate critical job responsibilities.	Interviewed the EVP of People and the Senior Director of People Operations and determined that formal job descriptions are maintained for critical roles	No Relevant Exceptions Noted

		Observed job descriptions and verified that the organization maintains job descriptions for critical roles that describe job-specific responsibilities	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	Heap performs background checks on employees prior to onboarding.	Reviewed the Employee Handbook and verified that employees must complete a background check prior to onboarding Interviewed the EVP of People and the Senior Director of People Operations and determined that all potential employees are required to successfully complete a background check prior to onboarding Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees completed a background check	No Relevant Exceptions Noted
CC1.4.2	Heap requires all employees to participate in HIPAA and security awareness training upon hire. Employees are required to complete security awareness training annually after hire and HIPAA training upon hire and every two years thereafter.	Reviewed the Human Resources Policies (dated March 2023) and verified that all employees must complete security awareness training upon onboarding and annually thereafter Interviewed the Compliance Manager and verified that the organization requires all employees to undergo security awareness training upon hire and annually thereafter Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees completed security awareness and privacy training and HIPAA awareness training during onboarding	No Relevant Exceptions Noted
CC1.4.3	Heap requires engineers to stay up to date on configurations standards.	Interviewed the Senior Software Engineer and determined that infrastructure personnel are required to stay up to date on best practices Reviewed the Security Guidelines for New Infrastructure and verified that	No Relevant Exceptions Noted

		Configuration standards must be based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that the organization maintains configuration standards based on NIST guidelines and CIS benchmarks Observed policy review tickets in Jira and verified that policies are reviewed annually	
CC1.4.4	Heap uses job descriptions to communicate critical job responsibilities.	Interviewed the EVP of People and the Senior Director of People Operations and determined that formal job descriptions are maintained for critical roles Observed job descriptions and verified that the organization maintains job descriptions for critical roles that describe job-specific responsibilities	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	Heap documents policy review responsibilities, which include reviewing the policies on at least an annual basis.	Reviewed the information security policies and verified that the Compliance Manager is responsible for facilitating annual policy reviews Interviewed the Compliance Manager and determined that policies are reviewed annually; the Compliance Manager assigns different managers and department heads a task in Jira to review, update, and approve the policies of which they are the process owner or the subject matter experts (SMEs) Observed policy review tickets in Jira and verified that the Compliance Manager facilitates annual review of policies by process owners and SMEs	No Relevant Exceptions Noted
CC1.5.2	On an annual basis, Heap employees acknowledge their information security responsibilities as part of their	Interviewed the EVP of People and the Senior Director of People Operations and determined that performance evaluations are performed twice per	No Relevant Exceptions Noted

	annual security training and performance review conversations.	year; during the evaluate, employees receive feedback from their peers and managers and rate themselves according to Heap's values and any personal goals Observed an example performance evaluation and verified that the organization has a process in place to provide feedback and evaluating employee performance	
CC1.5.3	Heap aligns internal control responsibilities with business objectives and communicates them to the company on a monthly basis.	Interviewed the CFO and the EVP of Product and determined that the organization maintains value statements, such as Ownership, Respectful Candor, and having a Growth Mindset, all of which have implications related to security and compliance Observed the website and verified that the organization documents value statements that are accessible on the site Interviewed the CFO and the EVP of Product and determined that monthly all-hands meetings are held Observed the Outlook calendar of the CFO and the EVP of Product and verified that monthly all-hands meetings are held	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Communication and Information			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	Heap does not require the collection of sensitive data, and Heap has detection algorithms built into its platform to detect and purge any sensitive data that may be collected incidentally.	Reviewed the Confidential Information Policies and verified that the organization defines requirements for the protection of confidential customer information Interviewed the Senior Software Engineer and the Compliance Manager and determined that the application, by design, does not collect any sensitive data and is intended to provide customers with analytics tools; any customer information that is collected is considered confidential and is handled according to policy	No Relevant Exceptions Noted
CC2.1.2	Heap maintains data flow diagrams to outline the flow of data throughout its production environment.	Observed the data flow diagram in the Architecture Diagrams document (dated February 13, 2023) and compared it against the service delivery description and verified that the organization maintains an up-to-date and accurate data flow diagram	No Relevant Exceptions Noted
CC2.1.3	Heap conducts an independent third-party penetration test for the Heap production platform on an annual basis.	Reviewed the Risk Management Policies (dated March 2023) and verified that the organization documents requirements for annual penetration testing Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that an annual penetration test is performed; any exploitable vulnerabilities identified during the test are remediated and the systems are retested Observed the last penetration test report for the testing period from January 25, 2023 through February	No Relevant Exceptions Noted

		8, 2023 and verified that the organization engages with a third-party security firm perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	
CC2.1.4	Heap conducts an independent third-party vulnerability assessment for the Heap web application on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual vulnerability scanning Interviewed the Senior Software Engineer and determined that the organization performs regular scanning, including an annual penetration test and weekly scans using AWS native tools such as Trusted Advisor Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	No Relevant Exceptions Noted
CC2.1.5	Heap implements formal logging and monitoring across the production platform to alert personnel around any security or availability issues.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems	No Relevant Exceptions Noted

		Interviewed the Senior Software Engineer and determined the following: • Event logging and monitoring is employed in the AWS production environment via AWS CloudTrail and Amazon CloudWatch • Datadog is used to monitor system capacity • Wazuh is used to monitor network traffic for suspicious activity • Logs are reviewed monthly in Kibana • Logs are retained for at least a year Observed a demonstration of Wazuh and AWS GuardDuty and verified that the organization has an intrusion detection system (IDS) in place on production systems Observed logs for various system monitoring tools and verified that logs were available throughout the audit period Observed security-related logs for CloudTrail stored in a read-only state and verified that security-related logs are stored in Amazon S3 and are retained for at least a year Observed application logs and verified that logs are stored in an encrypted S3 bucket for a rolling 14-day period Observed legacy application logs in Logz.io and verified that legacy application logs are archived for a rolling 14-day period Observed application logs in Wazuh and verified that application logs are archived for a rolling 14-day period	

		Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity Observed documentation from log reviews and verified that system activity logs are reviewed at least monthly	
CC2.1.6	Heap subscribes to various information sources, such as NIST, SANS, OWASP, and CIS, to keep themselves updated of emerging threats and vulnerabilities.	Reviewed the Security Guidelines for New Infrastructure and verified that Configuration standards must be based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that infrastructure personnel must stay up to date on best practices Interviewed the EVP of Engineering and the Senior Software Engineer and determined that the software development lifecycle (SDLC) integrates concepts from OWASP Observed notifications and emails that the Senior Software Engineer received and verified that the organization monitors industry accepted information sources such as SANS, NIST, OWASP, and CIS	No Relevant Exceptions Noted
CC2.1.7	Heap uses Datadog to monitor system capacity and related metrics on a continual basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined that Datadog is used to monitor system capacity Observed Datadog and verified that it is used to monitor system capacity and alerts personnel when thresholds are met	No Relevant Exceptions Noted

CC2.1.8	Heap performs vulnerability scans via AWS Trusted Advisor on a weekly basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that the organization monitors the native AWS benchmarking tool, AWS Trusted Advisor, and reviews reports weekly Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly	No Relevant Exceptions Noted
CC2.1.9	Heap conducts monitoring activities to evaluate the functioning of internal controls.	Observed a demonstration of the PagerDuty console and verified that the organization has systems and processes in place for monitoring the operating efficiency of the Heap analytics platform	No Relevant Exceptions Noted
CC2.1.10	Heap maintains network and systems diagrams to identify key systems and interfaces within the production environment.	Reviewed the System Development Policies and verified that engineers are responsible for maintaining an up-to-date network diagram Observed the network diagram in the Architecture Diagrams document (dated February 13, 2023) and compared it against the system inventory and service delivery description and verified that the organization maintains an up-to-date and accurate network diagram	No Relevant Exceptions Noted
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	Heap outlines the services it provides to its clients through contractual agreements and marketing materials.	Observed the client contract language and verified that the organization includes SLAs in the contract language that outlines the services the organization will provide to its clients during a business engagement	No Relevant Exceptions Noted
CC2.2.2	Heap uses job descriptions to communicate job responsibilities to critical positions within Heap.	Interviewed the EVP of People and the Senior Director of People Operations and determined that	No Relevant Exceptions Noted

		formal job descriptions are maintained for critical roles Observed job descriptions and verified that the organization maintains job descriptions for critical roles that describe job-specific responsibilities	
CC2.2.3	Heap requires all employees to participate in HIPAA and security awareness training upon hire. Employees are required to complete security awareness training annually after hire and HIPAA training upon hire and every two years thereafter.	Reviewed the Human Resources Policies (dated March 2023) and verified that all employees must complete security awareness training upon onboarding and annually thereafter Interviewed the Compliance Manager and verified that the organization requires all employees to undergo security awareness training upon hire and annually thereafter Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees completed security awareness and privacy training and HIPAA awareness training during onboarding	No Relevant Exceptions Noted
CC2.2.4	Heap subscribes to various information sources, such as NIST, SANS, OWASP, and CIS, to keep themselves updated of emerging threats and vulnerabilities.	Reviewed the Security Guidelines for New Infrastructure and verified that Configuration standards must be based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that infrastructure personnel are required to stay up to date on best practices Interviewed the EVP of Engineering and the Senior Software Engineer and determined that the SDLC integrates concepts from OWASP Observed notifications and emails that the Senior Software Engineer received and verified that the organization monitors industry	No Relevant Exceptions Noted

		accepted information sources such as SANS, NIST, OWASP, and CIS	
CC2.2.5	Heap has formally documented incident response policies and procedures in place that are reviewed on an annual basis.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Observed policy review tickets in Jira and verified that the organization's information security policies, including the Incident Management Policies, are reviewed annually	No Relevant Exceptions Noted
CC2.2.6	New members of the on-call team are paired with experienced team members when they first join the team to ensure they are thoroughly trained.	Reviewed the Incident Management Policies and verified that all on-call employees must be trained on incident response procedures Interviewed the Senior Software Engineer and verified that the organization leveraged a real incident that occurred during the audit period as a training opportunity for the on-call team Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the organization has incident response and reporting procedures in place to adequately identify and respond to security incidents and to document lessons learned	No Relevant Exceptions Noted
CC2.2.7	Heap has policies in place that describe how internal personnel should report security breaches.	Reviewed the Incident Management Policies and verified that procedures for communicating about suspected breaches are defined Observed policy review tickets in Jira and verified that the organization's information security policies are reviewed annually	No Relevant Exceptions Noted

CC2.2.8	Heap maintains information security policies for the production environment to support functioning of internal control and business objectives. These policies are available to all personnel on the company intranet.	Reviewed the following policies and verified that the organization maintains information security policies to support internal controls and business objectives: • Human Resources Policies • Policy Policies • Physical Security Policies • Logical Security Policies • Confidential Information Policies • System Operation Policies • Risk Management Policies • Third-Party Management Policies • Incident Management Policies • Business Continuity & Capacity Policies • Communication Policies • System Development Policies • Documentation Policies • Data Destruction Policies Interviewed the Compliance Manager and determined that information security policies are reviewed annually Observed policy review tickets in Jira and verified that the organization's information security policies are reviewed annually Interviewed the CFO and the EVP of Product and determined that monthly all-hands meetings are held Observed the Outlook calendar of the CFO and the EVP of Product and verified that monthly all-hands meetings are held Observed Confluence and BambooHR and verified that organizational policies are accessible to employees on the sites	No Relevant Exceptions Noted
CC2.2.9	Information security policies describe responsibilities for all employees.	Reviewed the following documents and verified that the organization maintains information security	No Relevant Exceptions Noted

		policies to support internal controls and business objectives, and policies communicate the information security responsibilities of all employees: • Human Resources Policies • Policy Policies • Physical Security Policies • Logical Security Policies • Confidential Information Policies • System Operation Policies • Risk Management Policies • Third-Party Management Policies • Incident Management Policies • Business Continuity & Capacity Policies • Communication Policies • System Development Policies • Documentation Policies • Data Destruction Policies Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that a security Slack channel is maintained where regular communication related to security and compliance is communicated to all employees Observed the security Slack channel and verified that it is used to regularly communicate security-related matters to employees	
CC2.2.10	Heap documents policy review responsibilities, which include reviewing the policies on at least an annual basis.	Interviewed the Compliance Manager and determined that information security policies are reviewed annually Observed policy review tickets in Jira and verified that the organization's information security policies are reviewed annually	No Relevant Exceptions Noted
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		

CC2.3.1	Heap communicates security, availability, and confidentiality requirements to its customers via contractual agreements and marketing materials.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Interviewed the Senior Software Engineer and determined the following: • All engineers participate in the incident response process as part of an on-call rotation • Production alerts trigger PagerDuty and Slack in channel #ops and have an attached Playbook for triage of the alert • If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist • Data breaches require specific steps as detailed in the Incident Management Policies Observed the client contract language and verified that the organization includes SLAs in the contract language Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	No Relevant Exceptions Noted
CC2.3.2	Heap has standard SLA language to offer clients upon request.	Observed the client contract language and verified that the organization includes SLAs in the contract language	No Relevant Exceptions Noted
CC2.3.3	Heap provides external users multiple methods of reporting security breaches, incidents, or other complaints.	Reviewed the Incident Management Policies and verified that the organization defines procedures for	No Relevant Exceptions Noted

		communicating suspected security incidents Interviewed the Compliance Manager and Senior Software Engineer and determined that personnel and clients have several channels available to report a suspected breach, including a dedicated email address Observed methods for clients and personnel to report suspected breaches or security incidents and verified the following: • The organization has a dedicated email address for external users to report suspected incidents • The organization's website displays contact information for Heap • Contact information for the legal department and the Data Privacy Officer are documented in the Privacy Policy	
CC2.3.4	Information security policies are distributed to authorized individuals outside the organization.	Reviewed the Documentation Policies and verified that the organization requires all information security policies to be treated as confidential and only distributed to business partners under NDA agreements Interviewed the Compliance Manager and determined that information security policies are distributed to external parties, such as business partners, who have business need to access the and who has signed an NDA Observed an example vendor NDA and verified that the organization requires vendors to sign an NDA prior to sharing confidential information	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Risk Assessment			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	Heap reviews various privacy regulatory requirements to align with company objectives.	Reviewed the Privacy Policy and verified that it addresses how personal information is handled in accordance with relevant legislation and regulations Observed the website and verified that the organization's Privacy Policy is accessible to third parties on the site	No Relevant Exceptions Noted
CC3.1.2	Heap performs risk assessments according to a documented methodology quarterly to ensure they are evaluating their ever-changing risk environment.	Reviewed the Risk Management Cadence (dated March 2023) and the Risk Management Policies and verified that the organization's risk assessment methodology is based on NIST standards Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to identify and submit risks via templated Jira tickets; managers review the existing risk register quarterly and any newly identified risks Observed the risk register in Jira and that the risk assessment reoccurs quarterly Observed Jira and verified that all risks are document as Jira tickets and are reviewed at least quarterly	No Relevant Exceptions Noted
CC3.2	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	Heap performs risk assessments according to a documented methodology quarterly to ensure they are evaluating their ever-changing risk environment.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that the organization's risk assessment methodology is based on NIST	No Relevant Exceptions Noted

		standards, and that risk assessments must be conducted quarterly Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to identify and submit risks via templated Jira tickets; managers review the existing risk register quarterly and any newly identified risks Observed the risk register in Jira and that the risk assessment reoccurs quarterly Observed Jira and verified that all risks are document as Jira tickets and are reviewed at least quarterly	
CC3.2.2	Heap documents the results of risk assessments in a risk assessment matrix that includes risk rating, strategies for managing identified risks, and ownership for any remediation needed.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that mitigating controls must be implemented based on each risk's overall risk ranking Interviewed the Compliance Manager and the Senior Software Engineer and determined that risks are ranked according to impact and likelihood and are assigned an overall risk ranking; mitigation plans are tracked in Jira with the highest severity risks being prioritized Observed the Jira tickets used to track remediation status and verified that risks are assigned a risk ranking based on their severity, and that high-ranking risks are prioritized for mitigation	No Relevant Exceptions Noted
CC3.2.3	Heap includes all information security and technology risks related to sensitive data and production platform in the risk registry. This includes any risk related to third-party tools or that can cause business disruption.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that the risk assessment is the responsibility of all employees, managers, and engineers Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to	No Relevant Exceptions Noted

		identify and submits risks via templated Jira tickets Observed the risk register in Jira and that the organization documents assets and threats to the confidentiality, integrity, and availability of the assets; threats are document in Jira tickets and assigned risk rankings where the impact value times the likelihood of occurrence equals the overall risk	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	Heap addresses the potential for fraud during biannual risk assessments.	Interviewed the Compliance Manager and the Senior Software Engineer and determined that risks related to fraud are documented in the risk register maintained in Jira Observed the risk register in Jira and verified that the organization documents risks associated with the potential for fraudulent use of Heap's platform	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	Heap includes all information security and technology risks related to sensitive data and production platform in the risk registry. This includes any risk related to third-party tools or that can cause business disruption.	Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to identify and submit risks via templated Jira tickets Observed the risk register in Jira and that the organization documents assets and threats to the confidentiality, integrity, and availability of the assets; threats are document in Jira tickets and assigned risk rankings where the impact value times the likelihood of occurrence equals the overall risk	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Monitoring Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC4.1	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	Heap performs vulnerability scans via AWS Trusted Advisor on a weekly basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that the organization monitors the native AWS benchmarking tool, AWS Trusted Advisor, and reviews reports weekly Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly	No Relevant Exceptions Noted
CC4.1.2	Heap implements formal logging and monitoring across the production platform to alert personnel around any security or availability issues.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined the following: • Event logging and monitoring is employed in the AWS production environment via AWS CloudTrail and Amazon CloudWatch • Datadog is used to monitor system capacity • Wazuh is used to monitor network traffic for suspicious activity • Logs are reviewed monthly in Kibana • Logs are retained for at least a year Observed a demonstration of Wazuh and AWS GuardDuty and verified that	No Relevant Exceptions Noted

		the organization has an IDS in place on production systems Observed logs for various system monitoring tools and verified that logs were available throughout the audit period Observed security-related logs for CloudTrail stored in a read-only state and verified that security-related logs are stored in Amazon S3 and are retained for at least a year Observed application logs and verified that logs are stored in an encrypted S3 bucket for a rolling 14-day period Observed legacy application logs in Logz.io and verified that legacy application logs are archived for a rolling 14-day period Observed application logs in Wazuh and verified that application logs are archived for a rolling 14-day period Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity Observed documentation from log reviews and verified that system activity logs are reviewed at least monthly	
CC4.1.3	Heap conducts an independent third-party penetration test for the Heap production platform on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual penetration testing Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that an annual penetration test is performed; any exploitable vulnerabilities identified during the test are remediated and the systems are retested	No Relevant Exceptions Noted

		Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	
CC4.1.4	Heap conducts an independent third-party vulnerability assessment for the Heap web application on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual vulnerability scanning Interviewed the Senior Software Engineer and determined that the organization performs regular scanning including an annual penetration test, and weekly scans using AWS native tools such as Trusted Advisor Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	No Relevant Exceptions Noted
CC4.1.5	Heap uses Datadog to monitor system capacity and related metrics on a continual basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems	No Relevant Exceptions Noted

		Interviewed the Senior Software Engineer and determined that Datadog is used to monitor system capacity Observed Datadog and verified that it is used to monitor system capacity and alerts personnel when thresholds are met	
CC4.1.6	On a quarterly basis, Heap performs a review of current user access to AWS production account and GitHub to verify access granted is appropriate.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the EVP of Engineering and the Senior Software Engineer and determined that source code is managed in GitHub; GitHub is used for code versioning Observed a demonstration of GitHub and verified that the organization uses it to manage source code and for version control Observed a demonstration of the use of role-based access in Okta and verified that personnel are granted access based on their job function	No Relevant Exceptions Noted
CC4.1.7	Heap performs risk assessments according to a documented methodology quarterly to ensure they are evaluating their ever-changing risk environment.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that the organization's risk assessment methodology is based on NIST standards Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to identify and submit risks via templated Jira tickets; managers review the existing risk register quarterly and any newly identified risks Observed the risk register in Jira and that the risk assessment reoccurs quarterly	No Relevant Exceptions Noted

		Observed Jira and verified that all risks are documented as Jira tickets and are reviewed at least quarterly	
CC4.1.8	Heap undergoes annual SOC 2 Type II audits.	Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that the organization undergoes SOC 2 Type II audits and reviews the results of the audit to evaluate findings and implement remediation Observed Jira tickets and verified that the organization tracks the remediation findings from annual audits using tickets	No Relevant Exceptions Noted
CC4.2	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	Heap provides updates regarding internal control performance to the board of directors on a quarterly basis.	Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that the organization has defined key performance indicators (KPIs) and objectives and key results (OKRs) for the various business units; these are reviewed regularly by management and during quarterly all-hands meetings Observed the organization's KPIs and OKRs and verified that they are defined for business units and are used to monitor operational quality and control Interviewed the CFO and the EVP of Product and determined that the management team meets weekly, and that monthly all-hands meetings are held Observed the Outlook calendar of the CFO and the EVP of Product and verified that various meetings are held with varying cadences Interviewed the CFO and the EVP of Product and determined that governance and oversight are provided	No Relevant Exceptions Noted

		by the board of directors, which meets quarterly Observed example board meeting minutes from a recent board meeting and verified that the board meets at least quarterly	
CC4.2.2	Heap documents the results of risk assessments in a risk assessment matrix that includes risk rating, strategies for managing identified risks, and ownership for any remediation needed.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that mitigating controls must be implemented based on each risk's overall risk ranking Interviewed the Compliance Manager and the Senior Software Engineer and determined that risks are ranked according to impact and likelihood and are assigned an overall risk ranking; mitigation plans are tracked in Jira with the highest severity risks being prioritized Observed the Jira tickets used to track remediation status and verified that risks are assigned a risk ranking based on their severity, and that high-ranking risks are prioritized for mitigation	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Control Activities			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC5.1	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	The duties of development, test, and production personnel are outlined in the System Development Policies.	Reviewed the System Development Policies (dated March 2023) and verified that the organization defines the responsibilities of development and test personnel and requires peer reviews be performed for each change prior to push to production Interviewed the EVP of Engineering and the Senior Software Engineer and determined that development, test, and production support are not distinct roles at Heap, and engineers have responsibilities across all three categories; policy dictates that development and system changes are reviewed by an engineer who is not the author to guarantee the independence of the review and feedback Observed a demonstration of the use of role-based access in Okta and verified that personnel are granted access based on their job function Interviewed the EVP of Engineering and the Senior Software Engineer and determined that peer review is enforced by workflows in GitHub Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that a peer review was performed on each sampled change prior to being pushed to production Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all developers are trained on OWASP Top 10 Vulnerabilities annually; a member of the security team conducts the training	No Relevant Exceptions Noted

		during a departmental all-hands meeting Observed the agenda and acknowledgements from the most recent secure code training and verified that the organization trains developers on secure coding techniques	
CC5.1.2	Heap documents the results of risk assessments in a risk assessment matrix that includes risk rating, strategies for managing identified risks, and ownership for any remediation needed.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that mitigating controls must be implemented based on each risk's overall risk ranking Interviewed the Compliance Manager and the Senior Software Engineer and determined that risks are ranked according to impact and likelihood and are assigned an overall risk ranking; mitigation plans are tracked in Jira with the highest severity risks being prioritized Observed the Jira tickets used to track remediation status and verified that risks are assigned a risk ranking based on their severity, and that high-ranking risks are prioritized for mitigation	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	Heap maintains information security policies for the production environment to support functioning of internal control and business objectives. These policies are available to all personnel on the company intranet.	Reviewed the following policies and verified that the organization maintains information security policies to support internal controls and business objectives: • Human Resources Policies • Policy Policies • Physical Security Policies • Logical Security Policies • Confidential Information Policies • System Operation Policies • Risk Management Policies • Third-Party Management Policies • Incident Management Policies • Business Continuity & Capacity Policies • Communication Policies	No Relevant Exceptions Noted

		• System Development Policies • Documentation Policies • Data Destruction Policies Interviewed the Compliance Manager and determined that information security policies are reviewed annually Observed policy review tickets in Jira and verified that the organization's information security policies are reviewed annually Interviewed the CFO and the EVP of Product and determined that monthly all-hands meetings are held Observed the Outlook calendar of the CFO and the EVP of Product and verified that monthly all-hands meetings are held Observed Confluence and BambooHR and verified that organizational policies are accessible to employees on the sites	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	Heap documents policy review responsibilities, which include reviewing the policies on at least an annual basis.	Reviewed the information security policies and verified that the Compliance Manager is responsible for facilitating annual policy reviews Interviewed the Compliance Manager and determined that policies are reviewed annually; the Compliance Manager assigns different managers and department heads a task in Jira to review, update, and approve the policies they are the process owner or SMEs of Observed policy review tickets in Jira and verified that the Compliance Manager facilitates annual review of policies by process owners and SMEs	No Relevant Exceptions Noted
CC5.3.2	Heap performs monitoring activities to ensure its policies are	Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that the organization	No Relevant Exceptions Noted

	being implemented to achieve its objectives.	undergoes SOC 2 Type II audits and reviews the results of the audit to evaluate findings and implement remediation Observed Jira tickets and verified that the organization tracks the remediation findings from annual audits using tickets Interviewed the Senior Software Engineer and the Data Protection Officer and determined that the organization has formally defined policies and procedures in place to prevent, detect, contain, and correct security violations Reviewed the information security policies and verified that the organization has implemented formal policies to prevent, detect, contain, and correct security violations Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that the organization has a disciplinary process in place for any policy violations including security-related policies; disciplinary measures are used based on the severity of the violation and include, but are not limited to, termination of employment Reviewed the Human Resources Policies and verified that the organization documents that disciplinary action up to and including termination if there is a violation of policies	

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Logical and Physical Access Controls			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	Heap uses AWS Key Management System (KMS) to manage encryption keys for backups and for exports of customer data.	Reviewed the Security Guidelines for New Infrastructure and verified that encryption keys for data at rest must be managed using AWS KMS Interviewed the Compliance Manager and the Senior Software Engineer and determined that encryption keys are generated and stored in AWS KMS; keys are automatically rotated by AWS Observed a demonstration of AWS KMS and verified that AWS keys are used to encrypt data at rest Observed Vault keys managed in Terraform and verified that the organization manages encryption keys according to industry-accepted best practices	No Relevant Exceptions Noted
CC6.1.2	Heap restricts access to the GitHub source code repository and implements version control.	Interviewed the EVP of Engineering and the Senior Software Engineer and determined that source code is managed in GitHub; GitHub is used for code versioning Observed a demonstration of GitHub and verified that the organization uses it to manage source code and for version control Observed a demonstration of the use of role-based access in Okta and verified that personnel are granted access based on their job function	No Relevant Exceptions Noted
CC6.1.3	Heap uses logical access control systems to restrict access to its systems.	Interviewed the Compliance Manager and determined that the organization uses Okta single sign-on to implement logical access to critical systems and	No Relevant Exceptions Noted

		uses AWS System Session Manager to facilitate remote access to production systems Observed a demonstration of an engineer logging into a production EC2 instance and verified that a VPN connection via AWS Client VPN is required, and authentication is integrated with Okta, which requires MFA; AWS System Session Manager is used to connect to the instance	
CC6.1.4	Heap implements the use of unique user IDs.	Interviewed the Compliance Manager and determined that users are assigned unique user IDs Observed onboarding documentation for a sample of 12 of 123 new hires and verified that all sampled employees were provided with a unique user ID	No Relevant Exceptions Noted
CC6.1.5	Heap has a Privacy Policy in place that addresses how personal information should be handled in accordance with relevant legislation and regulations.	Reviewed the Privacy Policy and verified that it describes the types of information collected and used by Heap, how data is collected and shared, how long data is retained, and addresses how personal information is handled in accordance with relevant legislation and regulations Observed the website and verified that the organization's Privacy Policy is accessible to third parties on the site	No Relevant Exceptions Noted
CC6.1.6	Access to production systems is restricted by giving access based on privileges or roles.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the Compliance Manager and determined that access is assigned to users based on the principle of least privilege, and users have only the access that their specific job responsibilities require Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges	No Relevant Exceptions Noted

		for all sampled personnel were appropriate for their job role Observed a demonstration of groups and users in Okta and verified that the organization implements role-based access Interviewed the Senior Software Engineer and determined that network settings are defined to only allow the minimum necessary traffic to the production environment Observed AWS security groups and verified that the organization limits network traffic to the minimum necessary	
CC6.1.7	Heap enforces the use of a VPN with multi-factor authentication (MFA) for remote access to its systems.	Interviewed the Compliance Manager and determined that the organization uses Okta single sign-on to implement logical access to critical systems and uses AWS System Session Manager to facilitate remote access to production systems Observed the AWS Client VPN and verified that it is integrated with Okta, and that VPN access is required to access production systems Observed a demonstration of Okta single sign-on and verified that MFA is required for all users Observed a demonstration of an engineer logging into production EC2 instance and verified that a VPN connection via AWS Client VPN is required, and authentication is integrated with Okta, which requires MFA; AWS System Session Manager is used to connect to the instance	No Relevant Exceptions Noted
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	Heap formally approves access to production systems prior to granting access.	Reviewed the Logical Security Policies (dated March 2023) and verified that the organization documents requirements related to logical access and granting account access to new employees Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges for all sampled personnel were appropriate for their job role	No Relevant Exceptions Noted
CC6.2.2	Access to production systems is restricted by giving access based on privileges or roles.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the Compliance Manager and determined that access is assigned to users based on the principle of least privilege, and users have only the access that their specific job responsibilities require Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges for all sampled personnel were appropriate for their job role Observed a demonstration of groups and users in Okta and verified that the organization implements role-based access Interviewed the Senior Software Engineer and determined that network settings are defined to only allow the minimum necessary traffic to the production environment Observed AWS security groups and verified that the organization limits network traffic to the minimum necessary	No Relevant Exceptions Noted
CC6.2.3	Heap revokes production access from terminated employees immediately.	Reviewed the Logical Security Policies and verified that employee access permissions must be revoked	No Relevant Exceptions Noted

		immediately upon termination of employment Interviewed the EVP of People and the Senior Director of People Operations and determined that account access is terminated at the end of the employee's last day (for voluntary terminations) and immediately upon termination (for involuntary terminations) Observed Okta for a sample of 14 of 144 terminated employees and verified that all sampled employees had their access revoked in a timely manner	
CC6.2.4	Heap facilitates hiring and termination procedures through checklists.	Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization uses an onboarding checklist to hire and onboard new employees Observed employee records for a sample of 12 of 123 new hires and verified that an onboarding checklist was completed for all sampled employees Interviewed the EVP of People and the Senior Director of People Operations and determined that the organization has the following processes in place for voluntary and involuntary terminations: • For voluntary terminations, HR is notified of the last date of employment and a ticket is submitted • For involuntary terminations, HR coordinates with IT to have the employee's account access revoked immediately upon notice of termination • BambooHR integrates with the IT ticketing system and creates a termination request Observed tickets for a sample of 14 of 144 terminated employees and verified	No Relevant Exceptions Noted

		that a termination ticket was submitted for all sampled former employees	
CC6.2.5	Heap employees authenticate to production systems using a username and password meeting minimum requirements and other account measures.	Reviewed the Logical Security Policies and verified that the organization requires that password policies be maintained and kept up to date Observed password parameters in Okta and verified that passwords must be at least eight characters long, complex, and expire after 180 days; accounts are configured to lock out for 15 minutes after five invalid log-in attempts Observed a demonstration of the password reset process and verified that users request a password reset from IT via Slack, the user's ID is confirmed via a separate channel of communication, and the password is reset to a randomly generated password that must be reset on the first login	No Relevant Exceptions Noted
CC6.2.6	Heap has formal procedures for registering and deregistering client users.	Interviewed the IT Director and determined that clients self-enroll, create an account, and receive a welcome email with links to provide a guided experience on how to install Heap's application; user access is disabled if the account is inactive for more than 30 days Observed the Okta users list and verified that all active user accounts had logged in the past 30 days	No Relevant Exceptions Noted
CC6.2.7	On a quarterly basis, Heap performs a review of current user access to AWS production account and GitHub to verify access granted is appropriate.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the EVP of Engineering and the Senior Software Engineer and determined that source code is managed in GitHub; GitHub is used for code versioning Observed a demonstration of GitHub and verified that the organization uses	No Relevant Exceptions Noted

		it to manage source code and for version control Observed a demonstration of the use of role-based access in Okta and verified that personnel are granted access based on their job function	
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	Heap formally approves access to production systems prior to granting access.	Reviewed the Logical Security Policies and verified that the organization documents requirements related to logical access and granting account access to new employees Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges for all sampled personnel were appropriate for their job role	No Relevant Exceptions Noted
CC6.3.2	Heap revokes production access from terminated employees immediately.	Reviewed the Logical Security Policies and verified that employee access permissions must be revoked immediately upon termination of employment Interviewed the EVP of People and the Senior Director of People Operations and determined that account access is terminated at the end of the employee's last day (for voluntary terminations) and immediately upon termination (for involuntary terminations) Observed Okta for a sample of 14 of 144 terminated employees and verified that all sampled employees had their access revoked in a timely manner	No Relevant Exceptions Noted
CC6.3.3	Heap employees authenticate to production systems using a username and password meeting minimum requirements and other account measures.	Reviewed the Logical Security Policies and verified that the organization requires that password policies be maintained and kept up to date	No Relevant Exceptions Noted

		Observed password parameters in Okta and verified that passwords must be at least eight characters long, complex, and expire after 180 days; accounts are configured to lock out for 15 minutes after five invalid log-in attempts Observed a demonstration of the password reset process and verified that users request a password reset from IT via Slack, the user's ID is confirmed via a separate channel of communication, and the password is reset to a randomly generated password that must be reset on the first login	
CC6.3.4	Access to production systems is restricted by giving access based on privileges or roles.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the Compliance Manager and determined that access is assigned to users based on the principle of least privilege, and users have only the access that their specific job responsibilities require Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges for all sampled personnel were appropriate for their job role Observed a demonstration of groups and users in Okta and verified that the organization implements role-based access Interviewed the Senior Software Engineer and determined that network settings are defined to only allow the minimum necessary traffic to the production environment Observed AWS security groups and verified that the organization limits network traffic to the minimum necessary	No Relevant Exceptions Noted

CC6.3.5	Heap enforces the use of a VPN with MFA for remote access to its systems.	Interviewed the Compliance Manager and determined that the organization uses Okta single sign-on to implement logical access to critical systems and uses AWS System Session Manager to facilitate remote access to production systems Observed the AWS Client VPN and verified that it is integrated with Okta, and that VPN access is required to access production systems Observed a demonstration of Okta single sign-on and verified that MFA is required for all users Observed a demonstration of an engineer logging into production EC2 instance and verified that a VPN connection via AWS Client VPN is required, and authentication is integrated with Okta, which requires MFA; AWS System Session Manager is used to connect to the instance	No Relevant Exceptions Noted
CC6.3.6	Heap implements the use of unique user IDs.	Interviewed the Compliance Manager and determined that users are assigned unique user IDs Observed onboarding documentation for a sample of 12 of 123 new hires and verified that all sampled employees were provided with a unique user ID	No Relevant Exceptions Noted
CC6.3.7	On a quarterly basis, Heap performs a review of current user access to AWS production accounts and GitHub to verify access granted is appropriate.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the EVP of Engineering and the Senior Software Engineer and determined that source code is managed in GitHub; GitHub is used for code versioning Observed a demonstration of GitHub and verified that the organization uses it to manage source code and for version control	No Relevant Exceptions Noted

		Observed a demonstration of the use of role-based access in Okta and verified that personnel are granted access based on their job function	
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	Heap restricts access to its physical office locations.	Reviewed the Physical Security Policies (dated March 2023) and verified that the organization must implement controls to restrict access to office facilities Interviewed the Compliance Manager and the IT Director and determined that access to the San Francisco and New York offices is restricted using a badge access control system Observed the San Francisco office and verified that badge access is required at every ingress point to the office Observed the New York office and verified that badge access is required at every ingress point to the office Observed physical access logs and verified that they are retained for a year Observed the badge access system records for a sample of 14 of 144 terminated employees and verified that all sampled former employees were removed from the access list for the offices	No Relevant Exceptions Noted
CC6.4.2	Heap performs daily scheduled backups of production data to AWS S3.	Reviewed the System Development Policies and verified that all client information must be backed up to cloud storage, and that the backups must be encrypted Interviewed the Senior Software Engineer and determined that RDS backups are performed nightly for all databases and are retained for six days; client data, Elasticsearch, and GitHub	No Relevant Exceptions Noted

		are backed up to S3 nightly and are retained at least three months Observed a demonstration of backups in AWS and verified that Amazon RDS backups are performed nightly for all databases and are retained for six days; client data, Elasticsearch, and GitHub are backed up to S3 nightly and are retained at least three months; and backups are encrypted	
CC6.4.3	Heap has implemented video surveillance cameras to monitor access to its physical office facilities.	Reviewed the Physical Security Policies and verified that Heap's offices must be equipped with security cameras to monitor the environment Interviewed the Compliance Manager and the IT Director and determined that the San Francisco and New York offices are equipped with security cameras Observed the San Francisco office and verified that security cameras were positioned at every ingress and egress point in the office, and that video footage is retained for at least 90 days Observed the New York office and verified that the office is in a multi-tenant building; security cameras operated by building management are in place to monitor ingress and egress points to the building and in the lobby and elevator areas	No Relevant Exceptions Noted
CC6.4.4	Heap prevents unauthorized access to its facilities by keeping all doors locked, implementing video surveillance, and employing visitor management procedures.	Reviewed the Physical Security Policies and verified that the organization documents requirements for physical security controls implemented in the San Francisco and New York offices Interviewed the Compliance Manager and the IT Director and determined that the physical security controls implemented in the San Francisco and New York offices include the following: • Access badges	No Relevant Exceptions Noted

		• Visitor registration process • Security cameras Interviewed the Compliance Manager and the IT Director and determined that physical controls are periodically inspected to ensure they are functioning as intended Observed the San Francisco office and verified that badge access is required at every ingress point to the office Observed the New York office and verified that badge access is required at every ingress point to the office Observed physical access logs and verified that they are retained for a year Observed badge access system and verified that network closets are restricted to IT and appropriate management employees Observed the San Francisco office and verified that the organization had a visitor registration process in place at the front desk Observed the New York office and verified that the organization had visitor registration process in place at the front desk Observed the San Francisco office and verified that security cameras were positioned at every ingress and egress point in the office, and that video footage is retained for at least 90 days Observed the New York office and verified that the office is in a multi-tenant building; security cameras operated by building management are in place to monitor ingress and egress points to the building and in the lobby and elevator areas	

CC6.4.5	Heap uses a visitor log that collects the visitor's full name, email address, and the person being visited.	Reviewed the Physical Security Policies and verified that visitors to Heap offices must sign in on a visitor's log Interviewed the Compliance Manager and the IT Director and determined that visitors are pre-approved and must sign into the visitor logs at the front desk upon arrival Observed the San Francisco office and verified that the organization had visitor registration process in place at the front desk Observed the New York office and verified that the organization had visitor registration process in place at the front desk Observed visitor logs and verified that visitor logs are maintained at least a year	No Relevant Exceptions Noted
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.		
CC6.5.1	Heap has policies in place that address secure media destruction requirements.	Reviewed the Data Destruction Policies and verified that the organization requires that laptops be wiped prior to destruction Interviewed the Compliance Manager and the IT Director and determined that computer equipment and media marked for destruction is held in secure storage where it is then wiped prior to disposal Observed the San Francisco and the New York offices and verified that laptops awaiting destruction and disposal are stored in the IT closet; the IT closets in both locations are locked with a physical key and can only be accessed by IT and the Office Manager	No Relevant Exceptions Noted
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		

CC6.6.1	Heap employs AWS best practices and Center for Internet Security (CIS) benchmarks to firewall their AWS production environment, and the San Francisco administrative office is protected with a firewall.	Reviewed the Security Guidelines for New Infrastructure and verified that Configuration standards must be based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that the organization maintains configuration standards based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that network settings are defined to only allow the minimum necessary traffic to the production environment Observed AWS security groups and verified that the organization limits network traffic to the minimum necessary	No Relevant Exceptions Noted
CC6.6.2	Access to production systems is restricted by giving access based on privileges or roles.	Reviewed the Logical Security Policies and verified that access is role-based and granted using the principle of least privilege Interviewed the Compliance Manager and determined that access is assigned to users based on the principle of least privilege, and users have only the access that their specific job responsibilities require Observed onboarding documentation for a sample of 12 of 123 new hires and verified that the access privileges for all sampled personnel were appropriate for their job role Observed a demonstration of groups and users in Okta and verified that the organization implements role-based access Interviewed the Senior Software Engineer and determined that network settings are defined to only allow the minimum necessary traffic to the production environment	No Relevant Exceptions Noted

		Observed AWS security groups and verified that the organization limits network traffic to the minimum necessary	
CC6.6.3	Heap encrypts sensitive data that is transmitted on public networks.	Reviewed the Confidential Information Policies and verified that the organization has policies in place regarding the implementation of encryption to protect sensitive data Interviewed the Compliance Manager and the Senior Software Engineer and determined that data in transit is encrypted with TLS 1.2 Observed the AWS client VPN and verified that VPN access is required to access production systems, and that data is encrypted with at least TLS 1.2 Observed AWS Elastic Load Balancer (ELB) configurations and verified that TLS 1.2 is enforced as the minimum acceptable protocol for encrypting data in transmission to the web application and APIs	No Relevant Exceptions Noted
CC6.6.4	Heap securely stores passwords and if passwords must be transmitted they are done so using TLS.	Reviewed the Confidential Information Policies and verified that the organization has policies in place regarding the implementation of encryption to protect sensitive data Observed logical access tools and verified that the organization uses Okta single sign-on, which encrypts password transmissions by default Observed AWS ELB configurations and verified that TLS 1.2 is enforced as the minimum acceptable protocol for encrypting data in transmission to the web application and APIs	No Relevant Exceptions Noted
CC6.6.5	Heap enforces the use of a VPN with MFA for remote access to its systems.	Interviewed the Compliance Manager and determined that the organization uses Okta single sign-on to implement logical access to critical systems and uses AWS System Session Manager to	No Relevant Exceptions Noted

		facilitate remote access to production systems Observed the AWS Client VPN and verified that it is integrated with Okta, and that VPN access is required to access production systems Observed a demonstration of Okta single sign-on and verified that MFA is required for all users Observed a demonstration of an engineer logging into production EC2 instance and verified that a VPN connection via AWS Client VPN is required, and authentication is integrated with Okta, which requires MFA; AWS System Session Manager is used to connect to the instance	
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	Heap encrypts sensitive data that is transmitted on public networks.	Reviewed the Confidential Information Policies and verified that the organization has policies in place regarding the implementation of encryption to protect sensitive data Interviewed the Compliance Manager and the Senior Software Engineer and determined that data in transit is encrypted with TLS 1.2 Observed the AWS client VPN and verified that VPN access is required to access production systems, and that data is encrypted with at least TLS 1.2 Observed AWS ELB configurations and verified that TLS 1.2 is enforced as the minimum acceptable protocol for encrypting data in transmission to the web application and APIs	No Relevant Exceptions Noted
CC6.7.2	Heap securely stores passwords, and, if passwords must be transmitted, the passwords are encrypted using TLS.	Reviewed the Confidential Information Policies and verified that the organization has policies in place regarding the implementation of encryption to protect sensitive data	No Relevant Exceptions Noted

		Observed logical access tools and verified that the organization uses Okta single sign-on, which encrypts password transmissions by default Observed AWS ELB configurations and verified that TLS 1.2 is enforced as the minimum acceptable protocol for encrypting data in transmission to the web application and APIs	
CC6.7.3	Heap uses AWS Certificate Manager to manage security certificates.	Interviewed the Senior Software Engineer and determined that the organization uses AWS Certificate Manager as an encrypted store for public TLS certificates Observed a demonstration of the AWS console and confirmed that AWS Certificate Manager is used to manage public TLS certificates	No Relevant Exceptions Noted
CC6.7.4	Heap protects information involved in application service transactions using encryption, and the Domain Name System (DNS) is locked to prevent misrouting.	Reviewed the Confidential Information Policies and verified that the organization has policies in place regarding the implementation of encryption to protect sensitive data Interviewed the Compliance Manager and the Senior Software Engineer and determined that data transmissions occur over encrypted connections to prevent misrouting Observed the AWS client VPN and verified that VPN access is required to access production systems, and that data is encrypted with at least TLS 1.2 Observed AWS ELB configurations and verified that TLS 1.2 is enforced as the minimum acceptable protocol for encrypting data in transmission to the web application and APIs	No Relevant Exceptions Noted
CC6.7.5	Heap development, testing, and production environments are all separate from one another.	Observed a demonstration of the organization's development and production environments and verified that development and production environments exist in separate AWS accounts, which are logically separated	No Relevant Exceptions Noted

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	All laptops have antivirus software enabled to protect against malicious software.	Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined the following: • The organization uses Wazuh IPS and FIM to perform continuous monitoring of production servers • Jamf antivirus is in place on all employee MacBooks • Windows Defender serves as the endpoint protection on all Windows 10 laptops Observed the Jamf console and verified the following: • All computers registered are equipped with the Jamf antivirus solution • Logs are retained in Jamf dashboard for at least a year • Scans are run daily • The Jamf agent is automatically updated Observed antivirus installation on the two Windows 10 laptops and verified that Windows Defender was enabled on both devices Observed the base AMI for all production EC2 instances and verified that the AMI includes the Wazuh agent for FIM and rootkit protection	No Relevant Exceptions Noted
CC6.8.2	Heap uses an open-source security solution as a host IDS.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined that Wazuh is used to monitor network traffic for suspicious activity Observed the base AMI for all production EC2 instances and verified that the AMI includes the Wazuh agent for FIM and rootkit protection	No Relevant Exceptions Noted

		Observed application logs in Wazuh and verified that application logs are archived for a rolling 14-day period	

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
System Operations			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	Heap uses configuration management and monitoring mechanisms to automatically apply configuration standards, which are based on NIST and CIS, to production systems.	Reviewed the Security Guidelines for New Infrastructure (dated March 2023) and verified that the organization requires the following: • Configuration standards must be based on NIST guidelines and CIS benchmarks • Personnel with configuration management responsibilities must stay up to date on best practices • Pre-configured AMIs and Terraform modules must be used whenever possible Interviewed the Senior Software Engineer and determined the following: • The organization uses infrastructure as code (IaC) to tear down and deploy infrastructure weekly • Servers are built from a golden AMI, which is updated monthly with the newest security patches and any configuration changes that are necessary • All critical infrastructure is built from golden AMIs and Terraform modules under version control and change management Observed the build image for golden AMIs for the production environment and verified that Wazuh agent is installed on each server Observed AWS and verified that most AWS EC2 instances are ephemeral	No Relevant Exceptions Noted

		Observed the repository of AMIs and verified that it was updated at least monthly throughout the audit period Observed the Jamf console and verified that OS updates are applied automatically	
CC7.1.2	Heap has formal Change Management policies and procedures in place to help engineers deploy changes in a secure manner.	Reviewed the System Development Policies and verified that the organization documents a software development lifecycle (SDLC) that guides the development and change management process Interviewed the EVP of Engineering and the Senior Software Engineer and determined that the SDLC integrates concepts from OWASP Interviewed the EVP of Engineering and the Senior Software Engineer and determined that source code is managed in GitHub; GitHub is used for code versioning Observed a demonstration of GitHub and verified that the organization uses it to manage source code and for version control Reviewed the System Development Policies and verified that peer reviews must be performed for each change prior to push to production Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all code changes are peer reviewed, which are enforced in GitHub before they are approved to merge to production; part of the code review process includes checking for OWASP Top 10 vulnerabilities Observed a demonstration of GitHub workflows and verified that various tools for static analysis are	No Relevant Exceptions Noted

		incorporated into the development process including the following: • Danger • ESLint • Checkov • Proto Lint • ShellCheck • Secret Linter Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that the following is documented for each sampled change: • Change tickets • Approval • Peer review • Impact analysis • Backout plans	
CC7.1.3	Heap executes independent code reviews before implementing changes into production environment.	Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all code changes are peer reviewed, which are enforced in GitHub before they are approved to merge to production Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that a peer review was performed on each sampled change prior to being pushed to production	No Relevant Exceptions Noted
CC7.1.4	Heap has formally documented vulnerability management policies and procedures.	Reviewed the System Operation Policies and verified that the organization has policies in place to guide the remediation of vulnerabilities Interviewed the EVP of Engineering and the Senior Software Engineer and determined that part of the code review process includes checking for OWASP Top 10 vulnerabilities Observed a demonstration of GitHub workflows and verified that various tools for static analysis are incorporated into the development process including the following: • Danger	No Relevant Exceptions Noted

		• ESLint • Checkov • Proto Lint • ShellCheck • Secret Linter	
CC7.1.5	Heap performs vulnerability scans via AWS Trusted Advisor on a weekly basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that the organization monitors the native AWS benchmarking tool, AWS Trusted Advisor, and reviews reports weekly Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly	No Relevant Exceptions Noted
CC7.1.6	Heap conducts an independent third-party penetration test for the Heap production platform on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual penetration testing Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that an annual penetration test is performed; any exploitable vulnerabilities identified during the test are remediated and the systems are retested Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were	No Relevant Exceptions Noted

		remediated, and the environment was retested	
CC7.1.7	Heap conducts an independent third-party vulnerability assessment for the Heap web application on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual vulnerability scanning Interviewed the Senior Software Engineer and determined that the organization performs regular scanning including an annual penetration test, and weekly scans using AWS native tools such as Trusted Advisor Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm to perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	No Relevant Exceptions Noted
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	Heap implements formal logging and monitoring across the production platform to alert personnel around any security or availability issues.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined the following: • Event logging and monitoring is employed in the AWS production environment via	No Relevant Exceptions Noted

		AWS CloudTrail and Amazon CloudWatch • Datadog is used to monitor system capacity • Wazuh is used to monitor network traffic for suspicious activity • Logs are reviewed monthly in Kibana • Logs are retained for at least a year Observed a demonstration of Wazuh and AWS GuardDuty and verified that the organization has an IDS in place on production systems Observed logs for various system monitoring tools and verified that logs were available throughout the audit period Observed security-related logs for CloudTrail stored in a read-only state and verified that security-related logs are stored in Amazon S3 and are retained for at least a year Observed application logs and verified that logs are stored in an encrypted S3 bucket for a rolling 14-day period Observed legacy application logs in Logz.io and verified that legacy application logs are archived for a rolling 14-day period Observed application logs in Wazuh and verified that application logs are archived for a rolling 14-day period Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity Observed documentation from log reviews and verified that system	

		activity logs are reviewed at least monthly	
CC7.2.2	Heap uses an open-source security solution as a host IDS.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined that Wazuh is used to monitor network traffic for suspicious activity Observed the base AMI for all production EC2 instances and verified that the AMI includes the Wazuh agent for FIM and rootkit protection Observed application logs in Wazuh and verified that application logs are archived for a rolling 14-day period	No Relevant Exceptions Noted
CC7.2.3	Heap implements formal logging and monitoring policies and procedures.	Reviewed the System Operation Policies and verified that system activity logs must be captured and reviewed for anomalies by engineers at least quarterly Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Observed system event logs and verified that logs, among other fields, contain the appropriate attributes, including but not limited to the following: • Source IP • Destination IP • Destination port • Protocol type (e.g., TCP, UDP, and ICMP) • Timestamp Observed documentation from log reviews and verified that system activity logs are reviewed at least monthly	No Relevant Exceptions Noted

		Observed a demonstration of FIM alerts in Wazuh integrated with PagerDuty and verified that the organization has change detection mechanisms in place for files Observed a demonstration of Wazuh and AWS GuardDuty and verified that the organization has IDS in place on production systems Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity	
CC7.2.4	Logs are required to contain specific information.	Reviewed the System Operation Policies and verified that system activity logs must be captured and reviewed for anomalies by engineers at least quarterly Observed system event logs and verified that logs, among other fields, contain the appropriate attributes, including but not limited to the following: • Source IP • Destination IP • Destination port • Protocol type (e.g., TCP, UDP, and ICMP) • Timestamp	No Relevant Exceptions Noted
CC7.2.5	The Incident Management Policies and the Systems Operation Policies describe how the following are monitored: • Alerts from intrusion detection and intrusion prevention (IDS/IPS) • Alerts from FIM systems • Detection of unauthorized wireless access points	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Observed a demonstration of FIM alerts in Wazuh integrated with PagerDuty and verified that the organization has change detection mechanisms in place for files Observed a demonstration of Wazuh and AWS GuardDuty and verified that the organization has IDS in place on production systems	No Relevant Exceptions Noted

		Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity	
CC7.2.6	The Incident Management Policies require that Heap monitor its systems for anomalies.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Observed a demonstration of FIM alerts in Wazuh integrated with PagerDuty and verified that the organization has change detection mechanisms in place for files Observed a demonstration of Wazuh and AWS GuardDuty and verified that the organization has IDS in place on production systems Observed a demonstration of PagerDuty and verified that it is integrated with Wazuh and AWS GuardDuty to produce alerts based on suspicious network activity	No Relevant Exceptions Noted
CC7.2.7	Heap uses Datadog to monitor system capacity and related metrics on a continual basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined that Datadog is used to monitor system capacity Observed Datadog and verified that it is used to monitor system capacity	No Relevant Exceptions Noted
CC7.2.8	Heap performs vulnerability scans via AWS Trusted Advisor on a weekly basis.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that the organization monitors the native AWS	No Relevant Exceptions Noted

		benchmarking tool, AWS Trusted Advisor, and reviews reports weekly Observed a demonstration of AWS and verified that the organization monitors AWS Trusted Advisor and reviews reports weekly	
CC7.2.9	Heap conducts an independent third-party penetration test for the Heap production platform on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual penetration testing Interviewed the Senior Software Engineer, the Director of IT, and the Compliance Manager and determined that an annual penetration test is performed; any exploitable vulnerabilities identified during the test are remediated and the systems are retested Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm to perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	No Relevant Exceptions Noted
CC7.2.10	Heap conducts an independent third-party vulnerability assessment for the Heap web application on an annual basis.	Reviewed the Risk Management Policies and verified that the organization documents requirements for annual vulnerability scanning Interviewed the Senior Software Engineer and determined that the organization performs regular scanning including an annual penetration test, and weekly scans using AWS native tools such as Trusted Advisor Observed a demonstration of AWS and verified that the organization	No Relevant Exceptions Noted

		monitors AWS Trusted Advisor and reviews reports weekly Observed the last penetration test report for the testing period from January 25, 2023 through February 8, 2023 and verified that the organization engages with a third-party security firm to perform a penetration test at least annually Observed the remediation penetration test report (dated March 16, 2023) and verified that all exploitable vulnerabilities were remediated, and the environment was retested	
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	Heap has Incident Management policies in place to guide personnel in reporting anomalies and other security-related incidents and concerns.	Reviewed the Incident Management Policies and verified that procedures for communicating about suspected breaches are defined Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	No Relevant Exceptions Noted
CC7.3.2	Heap has a formal Incident Management framework in place to identify, investigate, resolve, and monitor incidents affecting the availability, confidentiality, and security of production systems and data.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Interviewed the Senior Software Engineer and determined the following: • All engineers participate in the incident response process as part of an on-call rotation • Production alerts trigger PagerDuty and Slack in channel	No Relevant Exceptions Noted

		#ops and have an attached Playbook for triage of the alert • If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist • Data breaches require specific steps as detailed in the Incident Management Policies Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	
CC7.3.3	Heap documents incident recovery activities, including post-mortem activities. Corrective actions are implemented to prevent any future incidents.	Reviewed the Incident Management Policies and verified that an incident must be analyzed within a week of its occurrence to identify its root cause Observed an example of incident that required escalation and activation of the incident response procedures and verified that the organization has incident response and reporting procedures in place to adequately identify and respond to security incidents and to document lessons learned	No Relevant 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	Heap has a formal Incident Management framework in place to identify, investigate, resolve, and monitor incidents affecting the availability, confidentiality, and security of production systems and data.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Interviewed the Senior Software Engineer and determined the following:	No Relevant Exceptions Noted

		• All engineers participate in the incident response process as part of an on-call rotation • Production alerts trigger PagerDuty and Slack in channel #ops and have an attached Playbook for triage of the alert • If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist • Data breaches require specific steps as detailed in the Incident Management Policies Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	
CC7.4.2	Heap has Incident Management policies in place to guide personnel in reporting anomalies and other security-related incidents and concerns.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	No Relevant Exceptions Noted
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	Heap ensures that all laptop devices are monitored for security patching information and latest updates are applied in a timely manner.	Interviewed the Senior Software Engineer and determined that the organization uses IaC to tear down and deploy infrastructure weekly; servers are built from a golden AMI, which is updated monthly with the newest security patches and any necessary configuration changes	No Relevant Exceptions Noted

		Observed a demonstration of AWS Auto Scaling groups and verified that the base AMI was up to date with the most recent security patches Observed AWS and verified that most AWS EC2 instances are ephemeral Observed the repository of AMIs and verified that it was updated at least monthly throughout the audit period Observed the Jamf console and verified that OS updates are applied automatically Observed the patch status for both Windows laptops and verified that they are patched monthly	
CC7.5.2	Heap has a formal Incident Management framework in place to identify, investigate, resolve, and monitor incidents affecting the availability, confidentiality, and security of production systems and data.	Reviewed the Incident Management Policies and verified that the organization maintains procedures to identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Interviewed the Senior Software Engineer and determined the following: • All engineers participate in the incident response process as part of an on-call rotation • Production alerts trigger PagerDuty and Slack in channel #ops and have an attached Playbook for triage of the alert • If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist • Data breaches require specific steps as detailed in the Incident Management Policies	No Relevant Exceptions Noted

		Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	
CC7.5.3	Heap documents incident recovery activities, including post-mortem activities. Corrective actions are implemented to prevent any future incidents.	Reviewed the Incident Management Policies and verified that an incident must be analyzed within a week of its occurrence to identify its root cause Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the organization has incident response and reporting procedures in place to adequately identify and respond to security incidents and to document lessons learned	No Relevant Exceptions Noted

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Change Management			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
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	Heap uses configuration management and monitoring mechanisms to automatically apply configuration standards based on NIST and CIS to production systems.	Reviewed the Security Guidelines for New Infrastructure and verified that the organization requires the following: • Configuration standards must be based on NIST guidelines and CIS benchmarks • Personnel with configuration management responsibilities must stay up to date on best practices • Pre-configured AMIs and Terraform modules must be used whenever possible Interviewed the Senior Software Engineer and determined the following: • The organization uses IaC to tear down and deploy infrastructure weekly • Servers are built from a golden AMI, which is updated monthly with the newest security patches and any configuration changes that are necessary • All critical infrastructure is built from golden AMIs and Terraform modules under version control and change management Observed the build image for golden AMIs for the production environment and verified that Wazuh agent is installed on each server Observed AWS and verified that most AWS EC2 instances are ephemeral	No Relevant Exceptions Noted

		Observed the repository of AMIs and verified that it was updated at least monthly throughout the audit period Observed the Jamf console and verified that OS updates are applied automatically	
CC8.1.2	Heap has formal Change Management policies and procedures in place to help engineers deploy changes in a secure manner.	Reviewed the System Operation Policies and the System Development Policies and verified that all application, infrastructure, and network changes must be subject to version control and change management Observed documentation for a sample of 30 of 11,000 changes and verified that the organization requires change management, peer review, and approval on all network configuration changes	No Relevant Exceptions Noted
CC8.1.3	Heap references NIST and CIS as hardening standards for its system configurations.	Reviewed the Security Guidelines for New Infrastructure and verified that Configuration standards must be based on NIST guidelines and CIS benchmarks Interviewed the Senior Software Engineer and determined that the organization maintains configuration standards based on NIST guidelines and CIS benchmarks Observed policy review tickets in Jira and verified that policies are reviewed annually	No Relevant Exceptions Noted
CC8.1.4	Engineering managers are responsible for keeping configuration standards up to date.	Interviewed the Senior Software Engineer and determined that servers are built from a golden AMI, which is updated monthly with the newest security patches and any configuration changes that are necessary Observed Jira tickets and verified that the golden AMI is updated at least monthly	No Relevant Exceptions Noted

CC8.1.5	Heap executes independent code reviews before implementing changes into production environment.	Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all code changes are peer reviewed, which are enforced in GitHub before they are approved to merge to production Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that a peer review was performed on each sampled change prior to being pushed to production	No Relevant Exceptions Noted
CC8.1.6	Heap engineers test changes before implementing changes into production environment.	Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation Interviewed the EVP of Engineering and the Senior Software Engineer and determined that part of the code review process includes checking for OWASP Top 10 vulnerabilities Observed a demonstration of GitHub workflows and verified that various tools for static analysis are incorporated into the development process including the following: • Danger • ESLint • Checkov • Proto Lint • ShellCheck • Secret Linter	No Relevant Exceptions Noted
CC8.1.7	Heap development, testing, and production environments are all separate from one another.	Observed a demonstration of the organization's development and production environments and verified that development and production environments exist in separate AWS accounts, which are logically separated	No Relevant Exceptions Noted
CC8.1.8	Heap follows formal application change control procedures.	Reviewed the System Development Policies and verified that the organization documents an SDLC that	No Relevant Exceptions Noted

		guides the development and change management process Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that the following is documented for each sampled change: • Change tickets • Approval • Peer review • Impact analysis • Backout plans	

Trust Services Criteria for the Security, Availability, Confidentiality, and Processing Integrity Categories			
Risk Mitigation			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	Heap documents the results of risk assessments in a risk assessment matrix that includes risk rating, strategies for managing identified risks, and ownership for any remediation needed.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that mitigating controls must be implemented based on each risk's overall risk ranking Interviewed the Compliance Manager and the Senior Software Engineer and determined that risks are ranked according to impact and likelihood and are assigned an overall risk ranking; mitigation plans are tracked in Jira with the highest severity risks being prioritized Observed the Jira tickets used to track remediation status and verified that risks are assigned a risk ranking based on their severity, and that high-ranking risks are prioritized for mitigation	No Relevant Exceptions Noted
CC9.1.2	Heap performs risk assessments according to a documented methodology quarterly to ensure they are evaluating their ever-changing risk environment.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that the organization's risk assessment methodology is based on NIST standards Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization has a process in place for all employees to identify and submit risks via templated Jira tickets; managers review the existing risk register quarterly and any newly identified risks Observed the risk register in Jira and that the risk assessment reoccurs quarterly	No Relevant Exceptions Noted

		Observed Jira and verified that all risks are document as Jira tickets and are reviewed at least quarterly	
CC9.1.3	Heap reviews various regulatory requirements, company commitments, and compliance objectives to align with company objectives and include them in the risk assessment process.	Reviewed the Risk Management Cadence and the Risk Management Policies and verified that the organization's risk assessment methodology is based on NIST standards, and that risk assessments must be conducted quarterly Interviewed the Compliance Manager and the Senior Software Engineer and determined the following: • The organization has a process in place for all employees to identify and submit risks via templated Jira tickets • Managers review the existing risk register quarterly and any newly identified risks • Risks are ranked according to impact and likelihood and are assigned an overall risk ranking • Mitigation plans are tracked in Jira with the highest severity risks being prioritized Observed the risk register in Jira and that the risk assessment reoccurs quarterly Observed Jira and verified that all risks are documented as Jira tickets and are reviewed at least quarterly Observed the Jira tickets used to track remediation status and verified that risks are assigned a risk ranking based on their severity, and that high-ranking risks are prioritized for mitigation	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	Heap includes all information security and technology risks related to sensitive data and production platform in the risk registry. This includes any risk	Reviewed the Third-Party Management Policies (dated March 2023) and verified that the organization requires potential vendors be evaluated against criteria related to security, confidentiality, and	No Relevant Exceptions Noted

	related to third-party tools or that can cause business disruption.	availability prior to engaging their services Interviewed the Compliance Manager and determined that the organization uses a third-party tool to facilitate onboarding and monitoring of vendors; legal and compliance personnel perform reviews of new potential vendors prior to approval Observed a list of third parties and verified that the organization maintains a list of critical third-party service providers Observed a demonstration of the process for evaluating a new vendor and verified that the client has a process for approving new vendors, which includes a security review performed by the security and compliance team; the results of the review are documented in Jira	
CC9.2.2	Heap evaluates the compliance status of its vendors by obtaining and reviewing application audit reports on an annual basis.	Reviewed the Third-Party Management Policies and verified that vendors must be re-evaluated annually Interviewed the Compliance Manager and determined that existing vendors are reviewed annually via the collection of independent audit reports and/or security questionnaires Observed a demonstration of the process for re-evaluating existing vendors and verified that existing vendors are reviewed at least annually, and the results of the review are documented in Jira Observed vendor SOC 2 reports and verified that the organization collects independent audit reports for critical third parties (AWS, Datadog, and PagerDuty) at least annually	No Relevant Exceptions Noted
CC9.2.3	Heap communicates security, availability, and confidentiality requirements to its customers via	Reviewed the Incident Management Policies and verified that the organization maintains procedures to	No Relevant Exceptions Noted

	contractual agreements and marketing materials.	identify, investigate, resolve, and monitor for incidents that could affect the availability, confidentiality, and security of systems Interviewed the Senior Software Engineer and determined the following: • All engineers participate in the incident response process as part of an on-call rotation • Production alerts trigger PagerDuty and Slack in channel #ops and have an attached Playbook for triage of the alert • If the on-call engineer cannot resolve the issue with the contents of the Playbook alone, members of the team responsible for the affected sub-system may be paged manually to escalate and assist • Data breaches require specific steps as detailed in the Incident Management Policies Observed the client contract language and verified that the organization includes SLAs in the contract language Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	
CC9.2.4	Heap executes NDAs with third parties.	Reviewed the Third-Party Management Policies and verified that third parties are expected to adhere to confidentiality commitments Observed an example vendor NDA and verified that the organization requires vendors to sign an NDA	No Relevant Exceptions Noted

Additional Criteria for Availability			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	Heap uses Datadog to monitor system capacity and related metrics on a continual basis. Alerts are in place to notify for events that exceed thresholds.	Reviewed the Incident Management Policies and verified that it requires engineers to monitor the availability and security of systems Interviewed the Senior Software Engineer and determined that Datadog is used to monitor system capacity Observed Datadog and verified that it is used to monitor system capacity and alerts personnel when thresholds are met	No Relevant Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	Heap has a Continuity & Capacity Policies document that describes the plans to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.	Reviewed Heap Standard SLAs and verified that the organization commits to 99.5% availability annually Reviewed the Business Continuity & Capacity Policies (dated March 2023) and the Business Impact Analysis and verified that the organization formally documents plans to meet its SLAs Observed that the organization has a formal business continuity plan in place that includes the following: • Recovery response teams • List of critical components and software • Notifications and team responsibilities • IT restoration procedures • Requirements to retain evidence of plan maintenance • Management approval • Conditions for activating the plan • Awareness and education activities • Test schedule	No Relevant Exceptions Noted

		Reviewed the Business Continuity & Capacity Policies and the Business Impact Analysis and verified that the organization defines the recovery time objective (RTO) of 24 hours and the recovery point objective (RPO) of five minutes for critical business processes	
A1.2.2	Heap performs daily scheduled backups of production data to AWS S3.	Reviewed the System Development Policies and verified that all client information must be backed up to cloud storage, and that the backups must be encrypted Interviewed the Senior Software Engineer and determined that RDS backups are performed nightly for all databases and are retained for six days; client data, Elasticsearch, and GitHub are backed up to S3 nightly and are retained at least three months Observed a demonstration of backups in AWS and verified that Amazon RDS backups are performed nightly for all databases and are retained for six days; client data, Elasticsearch, and GitHub are backed up to S3 nightly and are retained at least three months; and backups are encrypted Interviewed the Compliance Manager and the Senior Software Engineer and determined that Redis, PostgreSQL databases, and S3 buckets are encrypted Observed the AWS console and verified that Amazon RDS and PostgreSQL databases are encrypted at rest; object storage in S3 is encrypted by default	No Relevant Exceptions Noted
A1.2.3	Backup processes have alerts configured to send notifications to personnel in case of failed backup status. Failure notifications are investigated and remediated, as necessary.	Reviewed the System Development Policies and verified that all client information must be backed up to cloud storage Interviewed the Senior Software Engineer and determined that RDS backups are performed nightly for all databases and are retained for six days; client data, Elasticsearch, and GitHub	No Relevant Exceptions Noted

		are backed up to S3 nightly and are retained at least three months Observed evidence from the last backup restoration test and verified that a backup restoration was successfully completed during the audit period Observed an example of incident that required escalation and activation of the Incident Management Policies and verified that the incident was investigated and resolved as required by the Incident Management Policies	
A1.2.4	Heap personnel perform restoration tests of backups on at least a quarterly basis when they have not occurred organically.	Observed evidence from the last backup restoration test and verified that a backup restoration was successfully completed during the audit period	No Relevant Exceptions Noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	Heap has formally documented backup policies and procedures.	Reviewed the System Development Policies and verified that all client information must be backed up to cloud storage, and that the backups must be encrypted Observed policy review tickets in Jira and verified that policies are reviewed annually by process	No Relevant Exceptions Noted
A1.3.2	Heap is required to test its business continuity plans at least annually.	Interviewed the Compliance Manager and the Senior Software Engineer and determined that the organization tests the business continuity and disaster recovery plan annually conducts annual tabletop test; the results of the test and lessons learned were documented Observed results of the most recent recovery test and verified that the organization performed a tabletop test of the business continuity and disaster recovery plan during the audit period, and that the lessons learned were documented within the test and corresponding remediation plans	No Relevant Exceptions Noted

Additional Criteria for Confidentiality			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Heap does not collect sensitive data; if sensitive data is collected incidentally, it is purged.	Reviewed the Confidential Information Policies and verified that the organization defines requirements for the protection of confidential customer information Interviewed the Senior Software Engineer and the Compliance Manager and determined that the application, by design, does not collect any sensitive data and is intended to provide customers with analytics tools; any customer information that is collected is considered confidential and is handled according to policy	No Relevant Exceptions Noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Heap has formal data destruction policies in place that require all confidential data to be wiped out of laptops before they are disposed of.	Reviewed the Data Destruction Policies and verified that the organization requires that laptops be wiped prior to destruction Interviewed the Compliance Manager and the IT Director and determined that computer equipment and media marked for destruction is held in secure storage where it is then wiped prior to disposal Observed the San Francisco and the New York offices and verified that laptops awaiting destruction and disposal are stored in the IT closet; the IT closets in both locations are locked with a physical key and can only be accessed by IT and the Office Manager	No Relevant Exceptions Noted

Additional Criteria for Processing Integrity			
Ctrl #	**Description of Controls**	**Service Auditor's Tests of Controls**	**Test Results**
PI1.1	The entity obtains or generates, uses, and communicates relevant, quality information regarding the objectives related to processing, including definitions of data processed and product and service specifications, to support the use of products and services.		
PI1.1.1	Employees acknowledge the information security policies and an acceptable use policy upon hire.	Interviewed the CFO, the EVP of Product, and the Compliance Manager and determined that employees are required to acknowledge an acceptable use policy and information security policies upon hire Observed employee records for a sample of 12 of 123 new hires and verified that all sampled employees acknowledge the information security policies, including an acceptable use policy	No Relevant Exceptions Noted
PI1.2	The entity implements policies and procedures over system inputs, including controls over completeness and accuracy, to result in products, services, and reporting to meet the entity's objectives.		
PI1.2.1	Heap's product integrates with client's webpages and applications to collect event data for processing and analysis.	Observed the Understand & Improve Digital Journeys slide deck and verified the following: • Heap's product can integrate with a client's webpages, Android applications, and iOS apps • Event listeners integrate with the client's application to ingest event data that is sent to Heap for processing • Event data is correlated with a user identity and stored in a PostgresSQL database cluster	No Relevant Exceptions Noted
PI1.2.2	Heap reviews and tests code changes prior to deployment to ensure the integrity of system inputs is maintained during processing.	Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all code changes are peer reviewed, which are enforced in GitHub before they are approved to merge to production	No Relevant Exceptions Noted

		Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that a peer review was performed on each sampled change prior to being pushed to production Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation Interviewed the EVP of Engineering and the Senior Software Engineer and determined that part of the code review process includes checking for OWASP Top 10 vulnerabilities Observed a demonstration of GitHub workflows and verified that various tools for static analysis are incorporated into the development process including the following: • Danger • ESLint • Checkov • Proto Lint • ShellCheck • Secret Linter	
PI1.3	The entity implements policies and procedures over system processing to result in products, services, and reporting to meet the entity's objectives.		
PI1.3.1	Heap's product correlates collected event data with a user's ID.	Observed the Understand & Improve Digital Journeys slide deck and verified the following: • Heap's product can integrate with a client's webpages, Android applications, and iOS apps • Event listeners integrate with the client's application to ingest event data that is sent to Heap for processing • Event data is correlated with a user identity and stored in a PostgresSQL database cluster	No Relevant Exceptions Noted
PI1.3.2	Heap reviews and tests code changes prior to deployment to ensure the processing integrity of the system is maintained.	Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation	No Relevant Exceptions Noted

		Interviewed the EVP of Engineering and the Senior Software Engineer and determined that all code changes are peer reviewed, which are enforced in GitHub before they are approved to merge to production Observed records for a sample of 30 of 11,000 pull requests in GitHub and verified that a peer review was performed on each sampled change prior to being pushed to production Reviewed the System Development Policies and verified that system changes must be reviewed for vulnerabilities prior to implementation Interviewed the EVP of Engineering and the Senior Software Engineer and determined that part of the code review process includes checking for OWASP Top 10 vulnerabilities Observed a demonstration of GitHub workflows and verified that various tools for static analysis are incorporated into the development process including the following: • Danger • ESLint • Checkov • Proto Lint • ShellCheck • Secret Linter	
PI1.4	The entity implements policies and procedures to make available or deliver output completely, accurately, and timely in accordance with specifications to meet the entity's objectives.		
PI1.4.1	Clients access and view data, define events, and perform analysis through the Heap SaaS front end.	Observed the Understand & Improve Digital Journeys slide deck and verified that clients can view event data, define events, and perform analysis through the front end of Heap's SaaS	No Relevant Exceptions Noted
PI1.4.2	Heap's product includes a function that allows clients to export their data to the client's data warehouse.	Observed the Understand & Improve Digital Journeys slide deck and verified the following:	No Relevant Exceptions Noted

		• Heap offers the ability to export data to client's data warehouses • When a client requests an export, their data is copied to S3 hourly where they can access via a cross account role in AWS to pull data to their warehouse • Supported warehouses include BigQ, Amazon Redshift, Snowflake, and Amazon S3 Observed a demonstration of backups in AWS and verified that client data is backed up to S3 nightly and is retained at least three months	
PI1.5	The entity implements policies and procedures to store inputs, items in processing, and outputs completely, accurately, and timely in accordance with system specifications to meet the entity's objectives.		
PI1.5.1	Heap has implemented policies and procedures for storing inputs and outputs completely, accurately, and in a timely manner.	Reviewed the System Development Policies and verified that all client information must be backed up to cloud storage, and that the backups must be encrypted Interviewed the Senior Software Engineer and determined that client data is backed up to S3 nightly and is retained at least three months Observed a demonstration of backups in AWS and verified that client data is backed up to S3 nightly and is retained at least three months Interviewed the Compliance Manager and the Senior Software Engineer and determined that Redis, PostgreSQL databases, and S3 buckets are encrypted Observed the AWS console and verified that Amazon RDS and PostgreSQL databases are encrypted at rest; object storage in S3 is encrypted by default	No Relevant Exceptions Noted