SYSTEM AND ORGANIZATION CONTROLS (SOC) 3 REPORT ON MANAGEMENT’S ASSERTION RELATED TO ITS

Continuous Code Improvement Platform

Relevant to Security, Availability and Confidentiality

For the period June 1, 2023 to May 31, 2024

TOGETHER WITH INDEPENDENT AUDITORS’ REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors’ Report

To the Management of Rollbar, Inc. (Rollbar)

Scope

We have examined Rollbar’s accompanying assertion titled “Assertion of Rollbar Management” (assertion) that the controls within Rollbar’s Continuous Code Improvement Platform (system) were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Rollbar’s service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (trust services criteria).*

Service Organization’s Responsibilities

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

Service Auditors’ Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management’s assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization’s service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management’s assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization’s service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Rollbar’s service commitments and system requirements based on the applicable trust services criteria.

- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Rollbar’s service commitments and system requirements based on the applicable trust services criteria.

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management’s assertion that the controls within Rollbar’s Continuous Code Improvement Platform were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Rollbar’s service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Sensiba LLP

San Jose, California

August 19, 2024

2. Assertion of Rollbar Management

We are responsible for designing, implementing, operating, and maintaining effective controls within the Rollbar, Inc. (Rollbar) Continuous Code Improvement Platform (system) throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Rollbar's service commitments and system requirements relevant to security, availability, and confidentiality were achieved. Our description of the boundaries of the system is presented in the section of this report titled, "Description of Rollbar's Continuous Code Improvement Platform," (description) and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Rollbar's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

Rollbar's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in the accompanying system description.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that the controls within the system were effective throughout the period June 1, 2023 to May 31, 2024, to provide reasonable assurance that Rollbar's service commitments and system requirements were achieved based on the applicable trust services criteria.

Signed by Rollbar Management

August 19, 2024

3. Description of Rollbar’s Continuous Code Improvement Platform

Rollbar, Inc. (Rollbar) was founded in 2012 with the objective of providing a Monitoring product for developers which helps them deliver high quality software quickly and painlessly. These solutions are delivered via a Software as a Service model. The organization is based in San Francisco, CA, with satellite offices in Barcelona and Budapest.

The Rollbar production environment has been developed to be consistent with the ISO 27001 standard.

Industries served by Rollbar include Financial Services, Telecommunications, Legal Services, Advertising, Manufacturing, Healthcare, Retail, Educational institutions, and Government agencies.

Services Provided

Rollbar provides Continuous Code Improvement Platform services to software developers which helps them deliver high quality software quickly and painlessly by providing them real-time visibility, proactive triaging, Root Cause Analysis, Application Instrumentation for various languages and platforms and seamless integrations with developer tools.

Rollbar’s core application is a cloud-based, multi-user, Software as a Service (SaaS) application. It enables processing of the following tasks related to software development:

Grouping Errors- Capturing and grouping occurrences of errors and messages into Items so that developers can accurately understand which are new vs. recurring, and the impact of each error (number of users affected, etc.).

Message Patterns - Rollbar has a database of well-known exception message patterns used by popular libraries and frameworks. Rollbar’s grouping algorithm recognizes these exception messages and considers the patterns when computing the fingerprint.

Reporting errors - Rollbar SDKs for popular programming languages and platforms provide one or more ways to capture and transmit errors via the Rollbar API.

Real-time Visibility - Rollbar supports several messaging and incident management tools where your team can get notified about errors and important events. Rollbar provides a finger printing service to improve signal-to-noise ratio.

Root Cause Analysis- Rollbar can trace all the data you need to debug, including request params, local var values, browsers, IPs, and more. Rollbar provides a Telemetry feature to retrace browser events leading up to an error.

Seamless Integration with Developer tools - Rollbar provides seamless integration with developer tools such as source code control system, issue management for proactive triaging, and People tracking.

Principal Service Commitments and System Requirements

Rollbar designs its processes and procedures related to their Continuous Code Improvement Platform services to meet its objectives for its customers, compliances, and employees. Those objectives are based on the service commitments that Rollbar makes to user entities, the laws and regulations that govern the provision of Continuous Code Improvement Platform services, and the financial, operational, and compliance requirements that Rollbar has established for the services. The Continuous Code Improvement Platform services of Rollbar are subject to the security and privacy requirements of ISO 27001 as well as the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Rollbar operates.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the Continuous Code Improvement Platform services that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit.

Rollbar establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Rollbar's system policies and procedures, system design documentation, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of the Continuous Code Improvement Platform services.

Components of the System

Infrastructure

The primary infrastructure used to provide Rollbar's Continuous Code Improvement Platform services system includes the following:

Primary Infrastructure		
Hardware	Type	Purpose
GCP Virtual Machines	Ubuntu 14.04/18.04 20.04/22.04	Run databases, caches, internal utilities
GKE Virtual Machines (managed by GCP)	1.24.12-gke.1000 or greater	Application code (web/api/workers)
GCP Load Balancers	External	Route customer traffic to both Kubernetes and VMs.
GCP MemoryStore	Redis	Caches customer data for application use.
GCP Kubernetes Engine	1.16.13-gke.401	Runs application code, internal tools and utilities.
GCP Dataproc	1.4.26-debian9	Runs data analytics jobs on customer data.

Software

The primary software used to provide Rollbar's Continuous Code Improvement Platform services system includes the following:

Primary Software		
Software	Operating System	Purpose
Linear	N/A	SDLC and Project Initiative management and tracking.
Zendesk	N/A	Ticketing system for reporting, tracking, and resolving customer issues and requests.
GitHub	N/A	Distributed version control system for tracking changes in source code during software development.
Statuspage	N/A	Online communication platform to inform customers of past and ongoing incidents, outages and performance issues
MailGun	N/A	Email marketing platform to send email programmatically in a safe and secure way
Superset	N/A	Platform to create and manage data pipeline with the goal of delivering business analytics and dashboards
DataDog	N/A	Monitoring system for all the different cloud components involved in our infrastructure
PagerDuty	N/A	Alerting system to automatically escalate incident response to the engineers on call
Amplitude	N/A	Business analytic platform with configurable dashboards, events and segmentation

Primary Software		
Software	Operating System	Purpose
Readme	N/A	Online documentation portal to host product documentation
Launch Darkly	N/A	Feature-flag platform to control progressive releases of new functionalities

People

Rollbar has a staff of approximately 25 employees organized in the following functional areas:

- Corporate. Executives, senior revenue operations staff, and company administrative support staff, such as training, accounting, finance, sales, marketing, human resources, and facilities. These individuals use the Rollbar software primarily as a tool to measure performance at an overall corporate level. This includes reporting done for internal metrics as well as for Rollbar's user entities.

- The software development staff develops and maintains the custom software for Rollbar. This includes the Rollbar application and associated SDKs, supporting utilities, and the external websites that interact with Rollbar. The staff includes software engineers, database administration, system administrators, User Interface Designers, Operations engineers and product/program managers.

- Customer Success staff collects customer requests directly from Rollbar users. These requests are entered into the customer support tool and get prioritized and addressed. In addition, customer success staff represents the voice of customers, maintains customer relationships and collects customer feedback and works with software development staff to increase customer satisfaction.

- IT. Help desk, IT infrastructure, IT system administration, Information Security & Compliance personnel manage electronic interfaces, security, compliance and business implementation support.

- The help desk group provides technical assistance to the Rollbar employees.
    - The information security staff supports Rollbar by monitoring internal and external security threats, obtaining and maintaining compliance, managing vendor security and maintaining security software.
    - The IT staff maintains the inventory of IT assets and manages the entire IT asset lifecycle including procurement, repair, and retirement.
    - The infrastructure, networking, and systems administration staff typically has no direct use of the Rollbar software. Rather, it supports Rollbar's IT infrastructure, which is used by the software. Operations engineers will deploy the releases of the Rollbar software and other dependent software into the production environment. This group does not directly use the Rollbar software, but it provides infrastructure

support, maintains business continuity as well as provides disaster recovery assistance.

Data

Data, as defined by Rollbar, constitutes the following:

- User and organization account metadata
- Raw data provided by customers.
- Logs of internal systems
- Internal monitoring data related to infrastructure operations.
- Internal documentation

Users sign up to the SaaS product through a web interface and configure their accounts for the team and organization. Customers then integrate the Rollbar SDK with their codebase resulting in their applications sending the Rollbar SaaS product information about errors and log events that are happening in the Customer's applications. This data is received by the SaaS product, processed, indexed into various databases and made available to the Rollbar Web Application to provide the Continuous Code Improvement Platform. Customer Success staff collects customer requests directly from Rollbar users. These requests are entered into the customer support tool and get prioritized and addressed. In addition, customer success staff represents the voice of customers, maintains customer relationships and collects customer feedback and works with software development staff to increase customer satisfaction.

Internal databases, virtual machines, and logs are only accessible by employees who require access in order to fulfill their role. Access to customer data is only provided to employees after they have received the required HIPAA training and only through secure mechanisms such as VPN tunnels.

Internal documentation is available for all full-time employees and is stored and maintained in 3rd party services such as Google Drive, and other SaaS solutions.

Processes, Policies and Procedures

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

Physical Security

All data is hosted by Google Cloud Platform (GCP). GCP data centers do not allow Rollbar employees physical access.

Logical Access

Rollbar uses role-based security architecture managed by IAM roles and adheres to the principle of least privilege. To secure our production environment we govern sudo privileges, SSH access, and VPN via role- based groups and enforcement of multi-factor authentication.

The VPN provides the gateway to all of our production infrastructure. VPN is authenticated via user ID, password, and multi-factor authentication (TOTP and mobile push notifications). SSH access via key- certificate pair is additionally verified by role-based groups to selected bastion hosts as a backup to VPN access.

Similarly, sudo access (and the sudo password) is restricted. Accounts have standard password configuration around rotation, strength, etc. Accounts are locked out after a number of incorrect attempts. Any user can be locked out of our production systems easily by removing/disabling their account.

Upon hire, employees receive access to Identity and Authentication management systems. Access modifications are performed by the internal IT team, as well as the Platform/Infrastructure team. All accounts are deactivated when an employee leaves the company, via requests generated by HR sent to Platform and IT. Role-based access and the provisioning of new roles is governed by a group of several people including Platform, Security, IT and HR.

Computer Operations – Backups

Rollbar ensures all customer data is backed up via GCP disk snapshots, and automatically validated on a schedule.

Every database cluster has a live replica as well as a backup host. This backup host replicates from the cluster master, and every 2 hours shuts itself down to snapshot its data volume.

These snapshots are saved at 2hr increments for 20hrs, and daily snapshots are saved for 7 days. An internal restore host automatically loads these snapshots every 2 hours and validates their contents are not corrupted.

Computer Operations – Availability

Rollbar monitors the capacity utilization for computing infrastructure through a number of monitoring tools:

- Prometheus/Graphite/Datadog
- Sensu/Pagerduty
- Stackdriver

For most computing resources additional capacity is provisioned by adding or upsizing servers. We do this via Terraform and can increase capacity with little difficulty as all of our infrastructure runs on cloud computing.

For all of our services that run on GCPs Kubernetes Engine, additional capacity is added within minutes by on-call engineers to respond to customer demand. Our node pools auto scale, so requests for additional capacity adds or removes servers without need for intervention.

In regard to patching, we utilize Tenable internally to monitor our provisioned infrastructure and alert us when systems need to be patched. We then utilize Ansible to patch the target infrastructure. For all of our Kubernetes infrastructure, we automatically upgrade our nodes whenever there is an update available. This ensures that our Kubernetes and VM environments are patched promptly.

Change Control

Rollbar utilizes a standard change control system, powered by Linear and GitHub.

We have documented life cycle policies and procedures to govern application and infrastructure changes. A ticketing system through Linear documents changes to the application and infrastructure. Runbooks and Procedures are created in Notion. Changes are validated in our staging environment before being run against production, which is totally separated from our production environment.

GitHub acts as our version control software. Through the widespread use of Infrastructure as Code products (Ansible and Terraform), our GitHub repos contain not only our application code but our infrastructure configuration. All changes are subject to code review, with specific groups of reviewers being necessary for changes to specific systems.

As mentioned earlier, Tenable monitors our systems to ensure patching compliance. Alerts raised by Tenable are patched via Ansible, with the change being reviewed and rolled out by the Platform team.

Data Communications

Rollbar protects its production infrastructure via GCP firewall rules. These firewall rules are actively maintained and enforced across all GCP projects.

All access to production systems is gated by our VPN. Access to the VPN is authenticated via user ID, password, and multi-factor authentication (TOTP and mobile push notifications).

Redundancy is built into all of our systems by distributing clusters across multiple availability zones, ensuring that if an AZ in GCP goes down we still maintain functionality. In addition, all of our data stores have replicas that can support full production load, so any failure to one of these data stores can be remediated by failover.

Penetration testing is conducted on a quarterly basis, with a variety of security researchers conducting the tests to ensure maximum coverage. Any issues found by penetration testing are remediated on schedule depending on the severity of the vulnerability.

Tenable and Jamf also provide constant monitoring of systems to ensure vulnerabilities are alerted on and remediated. Jamf provides a suite of security tools used for comprehensive monitoring and alerting. Certification Automation is utilized to provide automated security and compliance around Rollbar controls.

Boundaries of the System

The scope of this report includes the Continuous Code Improvement Platform services system performed in the US based Rollbar facilities. This report does not include the data center hosting services provided by GCP.

The applicable trust services criteria and the related controls:

Common Criteria (Security)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. 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

Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it 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). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). 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. For example, the information may be proprietary, intended only for entity personnel.

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.

Control Environment

Integrity and Ethical Values

Rollbar maintains four core values: honesty, transparency, dependability, and pragmatism, which serve as the foundation for the company’s behavioral standards. These core values are stated company-wide at monthly All Hands meeting and discussed in depth throughout the year to remind employees of their importance to the company and its success.

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

- Formally communicate entity values to all employees at bi-monthly company meetings.
- The Rollbar Company Handbook defines the company codes of conduct, business ethics, and communicates the general requirements and areas that would result in conflicts of interest. The Company Handbook is updated periodically and is always available for reference on the Notion page and HRIS system during onboarding.
- Policies and procedures require employees to sign an acknowledgment form indicating they have given consent to background checks which are performed as a component of the hiring process. Background checks are a component of onboarding and are initiated after the employment agreement is formally signed.
- Company Proprietary Information and Invention Agreement is acknowledged and signed by employees which is also performed as a component of the hiring process.

Commitment to Competence

Rollbar's management defines the required skills necessary to accomplish tasks that define an employee's role and core competency. Management considers the core skill level for all employee roles and job functions.

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

- Rollbar Management has considered the competence levels for particular roles. Job descriptions are crafted to include specifics of the required skill set, level of experience, education, and years of industry experience.
- Rollbar Management utilizes technical and cognitive testing for certain positions during the hiring process.

Management's Philosophy and Operating Style

Rollbar's management philosophy is built upon the mission to operate within a team-oriented environment. Leadership strives to maintain open and transparent communications with all employees regarding operations and performance.

Rollbar's management philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the approach to taking and monitoring business risks; attitudes and actions toward financial reporting; use of policies and procedures; and emphasis on planning and meeting budget, profit, and other financial and operating goals.

Specific control activities that Rollbar has implemented in this area are described below:

- Rollbar Leadership Team meetings are held every week to openly discuss operational planning and budgeting, human resource planning and hiring, customer related issues, and major initiatives and risks that affect the business as a whole. In addition, a quarterly offsite is held between Leadership to organize and implement future projects. Agendas and minutes from all Rollbar management meetings are recorded and communicated to relevant personnel.
- Rollbar management is periodically briefed on regulatory and industry changes affecting services provided.

Organizational Structure and Assignment of Authority and Responsibility

Rollbar's organizational structure provides the framework within which its activities for achieving entity- wide objectives are planned, executed, controlled, and monitored.

Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Specific control activities that Rollbar has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees during onboarding and are continually updated as needed.
- Organization charts are available for company-wide view through the HRIS system.
- Rollbar's operating goals and objectives are communicated to the entire organization during monthly All Hands meetings, employee performance reviews, and other written communications.

Human Resource Policies and Practices

Rollbar's People Team supports policies and practices to ensure Rollbar meets and exceeds hiring standards and maintains maximal employee engagement and retention. This function serves new hire pre-boarding and onboarding, in addition to existing employee evaluation, career progression, and biannual reviews.

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

- New employees are required to submit a background check and sign the company Proprietary Information and Inventions Agreement (PIIA) ahead of first day of employment with Rollbar
- Company policies including clean desk policy, security policy, and company asset policy are shared and new hires sign acknowledgements during initial onboarding.

- Evaluations for each employee are performed on a biannual basis.
- Company periodically audits compensation using market rate data and makes any necessary adjustments.
- Employee termination procedures are in place to guide the termination process and are documented in a termination workflow and checklist that is coordinated between the hiring manager, HR and IT.
- New hires and existing employees are periodically trained and retrained on the topic of Workplace Harassment and HIPAA.

Risk Assessment Process

Rollbar's risk assessment process identifies and manages risks that could potentially affect Rollbar's ability to provide reliable services to user organizations. This ongoing process requires that management identify significant risks inherent in products or services as they oversee their areas of responsibility. Rollbar identifies the underlying sources of risk, measures the impact to the organization, establishes acceptable risk tolerance levels, and implements appropriate measures to monitor and manage the risks.

This process has identified risks resulting from the nature of the services provided by Rollbar, and management has implemented various measures designed to manage these risks. Risks identified in this process include the following:

- Operational risk – changes in the environment, staff, or management personnel
- Strategic risk - new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory changes

Rollbar has assigned Information Security for identifying security and compliance risks to the entity and monitoring the operation of the firm's internal controls. The approach is intended to align the entity's strategy more closely with its key stakeholders, assist the organizational units with managing uncertainty more effectively, minimize threats to the business, and maximize its opportunities in the rapidly changing market environment. Rollbar attempts to actively identify and mitigate significant risks through the implementation of various initiatives and continuous communication with other leadership committees and senior management. Rollbar has created a Risk Assessment & Management Program which includes Risk Assessment & Management Policy.

Integration with Risk Assessment

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

Information and Communications Systems

Information and communication is an integral component of Rollbar's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. This process encompasses the primary classes of transactions of the organization, including the dependence on, and complexity of, information technology. At Rollbar, information is identified, captured, processed, and reported by various information systems, as well as through conversations with clients, vendors, regulators, and employees.

Departmental, functional, and project specific meetings are held to discuss operational efficiencies within the applicable areas and to disseminate new policies, procedures, controls, and other strategic initiatives within the organization. Additionally, all hands meetings are held every month to provide employees with updates on the company and key initiatives affecting the organization and its employees. Senior executives lead the All Hands meetings with information gathered from formal automated information systems and informal databases, as well as questions and conversations with colleagues. General updates to entity-wide security policies and procedures are usually communicated to the appropriate Rollbar personnel via email and instant messages.

Specific information systems used to support the Rollbar software are described in the Description of Services section above.

Monitoring Controls

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

On-Going Monitoring

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

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

Reporting Deficiencies

Rollbar is using Linear to document and track the results of on going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the Linear tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date. Rollbar did replace Shortcut with Linear, Periscope with Superset and Quip with Notion.

Incidents in the Last 12 Months

On September 6th, 2023, a threat actor accessed data in Rollbar's data warehouse. The data accessed included account names, usernames and email addresses, project and environment names, project configuration, project access tokens, and some item title data. There was no evidence that any of the project access tokens were used by the threat actor. However, out of caution, we expired all affected private project access tokens.

On January 8th, 2024 Rollbar experienced a technical incident as a result of conducting database maintenance. The technical incident began at 11:44 PST and was resolved by 14:30 PST. A data exposure between Rollbar’s customers occurred due to an internal system error, which was triggered during a database maintenance operation. As such a customer could potentially have seen another customer's data. All affected customers were notified. The root cause was related to caching. All affected data was removed and is no longer available via the Rollbar service.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Rollbar’s Continuous Code Improvement Platform.

Subservice Organizations

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

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

Security Category	
Criteria	*Controls expected to be in place*
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.	GCP is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
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.	
CC6.3 - 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.	
CC6.5 - 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.	

Security Category	
Criteria	*Controls expected to be in place*
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
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.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	GCP is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
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.	GCP is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

Rollbar, Inc. management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Rollbar, Inc. performs monitoring of the subservice organization controls, including the following procedures.

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

Complementary User Entity Controls

Rollbar’s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the SOC 2 Criteria related to Rollbar’s services to be solely achieved by Rollbar‘s control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Rollbar’s.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the SOC 2 Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities’ locations, user entities’ auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

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