

Vibemonitor, Inc.

System and Organization Controls (SOC) 2 Report

Beryl Software Reliability Platform

For the Period April 2, 2026 - July 2, 2026

Advantage PARTNERS

Table of Contents

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT 5
SECTION II: MANAGEMENT'S ASSERTION 11
SECTION III: DESCRIPTION OF THE SYSTEM 14
SECTION IV: DESCRIPTION OF CRITERIA, SERVICE AUDITOR TESTING 30

Executive Summary

Vibemonitor, Inc. - Beryl Software Reliability Platform

Scope	**Beryl Software Reliability Platform**
Period of Examination	April 2, 2026 to July 2, 2026
Subservice Providers	Amazon Web Service (AWS), Google Cloud Platform (GCP)
Opinion Result	Unqualified
Testing Exceptions	No Exceptions Noted
Complementary Subservice Organization Controls	Yes – See **Page 26**
Complementary User Entity Controls	Yes – See **Page 27**

Section I: Independent Service Auditor's Report



Advantage Partners
Seattle, WA

Section I: Independent Service Auditor's Report

To: Management of Vibemonitor, Inc.

Scope

We have examined the description of the system for Vibemonitor, Inc. ("Beryl" or the "Service Organization") of its Beryl Software Reliability Platform throughout the period April 2, 2026 to July 2, 2026 (the "description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* in AICPA*, Description Criteria* ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 2, 2026 to July 2, 2026, to provide reasonable assurance that Beryl's service commitments and system requirements were achieved based on the trust services criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, 2017 *Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

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

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Beryl, to achieve Beryl's service commitments and system requirements based on the applicable trust services criteria. The Description presents Beryl's controls; the applicable trust services criteria; and the complementary user entity controls assumed in the design of Beryl's controls. The description does not extend to the controls of the user entity.

Service Organization's Responsibilities

The Service Organization 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 Service Organization's service commitments and system requirements were achieved. The Service Organization has provided the accompanying assertion, "Management's Assertion" in **Section II**, ("assertion") about the description and the suitability of design and operating effectiveness of controls stated therein. The Service Organization 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 the design and operating effectiveness of the controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants (AICPA). 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 operating 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 those 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;

- Evaluating the overall presentation of the description.

- 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

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

Service Auditor's Independence and Quality Control

We have complied with the independence and other ethical requirements of the *Code of Professional Conduct* established by the AICPA. We applied the statements on quality control standards established by the AICPA, and accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

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

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

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

Description of Tests of Controls

The specific controls we tested, and the nature, timing, and results of our tests are listed in **Section IV** of this report.

Opinion

In our opinion, in all material respects,

a. The description fairly presents the Beryl Software Reliability Platform systems of Beryl that was designed and implemented throughout the period April 2, 2026 to July 2, 2026 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 2, 2026 to July 2, 2026, to provide reasonable assurance that Beryl's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization applied the complementary controls assumed in the design of the Service Organization's controls throughout that period.

c. The controls stated in the description operated effectively throughout the period April 2, 2026 to July 2, 2026, to provide reasonable assurance that Beryl's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of the Service Organization'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 Beryl, user entities of the in-scope services for Beryl's Beryl Software Reliability Platform systems during some or all of the period April 2, 2026 to July 2, 2026, business partners of Beryl subject to risks arising from interactions with Beryl 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 they interact with related controls at the Service Organization to achieve the Service Organization's 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.

Advantage Partners

August 26, 2026

Section II:
Management's Assertion

Section II: Management's Assertion

Assertion of Beryl's Management

We have prepared the accompanying description of the Beryl Software Reliability Platform system in **Section III** of Beryl ("Service Organization") throughout the period April 2, 2026 to July 2, 2026 (the "period"), 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, in AICPA Description Criteria, ("description criteria"). The description is intended to provide users with information about Beryl's system that may be useful when assessing the risks arising from interactions with Beryl system, particularly information about system controls that Beryl has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust service criteria relevant to security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* ("trust services criteria").

The Service Organization uses subservice organizations listed in **Section III** to support its overall system. The description indicates that the complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with the controls at Beryl, to achieve the service commitments and system requirements based on the applicable trust service criteria. The description presents Beryl's controls, the applicable trust service criteria, and the complementary subservice organization controls assumed in the design of Beryl's controls. The description does not disclose the actual controls at the subservice organization.

The Description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Beryl, to achieve Beryl's service commitments and system requirements based on the applicable trust services criteria. The Description presents Beryl's controls; the applicable trust services criteria; and the complementary user entity controls assumed in the design of Beryl's controls. The description does not extend to the controls of the user entity.

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

a. The description presents Beryl's system that was designed and implemented throughout the period of April 2, 2026 to July 2, 2026 in accordance with the description criteria.

b. The controls stated in the description were suitably designed throughout the period April 2, 2026 to July 2, 2026 to provide reasonable assurance that Beryl's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout

that period and if the subservice organization applied the complementary controls assumed in the design of Beryl's controls throughout the period.

c. The controls stated in the description operated effectively throughout the period of April 2, 2026 to July 2, 2026 to provide reasonable assurance that Beryl's service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls assumed in the design of Beryl's controls operated effectively throughout that period.

Section III:
Description of the System

Section III: Description of the System

Company Background

Beryl, an AI-powered Software Reliability Platform designed to help engineering teams maintain software reliability across the full lifecycle — proactively validating and monitoring their software, detecting issues, investigating live incidents, and tracking actions to resolution. Founded in 2025, the company is headquartered in San Francisco, California. All employees of the company are engaged and employed through its fully owned subsidiary, Greenfield Labs Private Limited, based in India, ensuring that all personnel supporting the system are formally structured within the scope of this review.

Description of Services Overview

Beryl is an AI-powered Software as a Service (SaaS) Software Reliability Platform offered by Beryl The system is designed to help software engineering teams maintain software reliability across the full lifecycle — proactively validating and monitoring their software, detecting issues and telemetry gaps, investigating live incidents, and tracking actions to resolution. The platform combines deterministic analysis with LLM-powered reasoning over codebase context and live telemetry.

The platform's core capabilities include the following. Specific features and user experience evolve continuously based on customer experimentation and product iteration:

- Automated Reliability Testing & Monitoring: Automated, recurring validation and monitoring of customer software, generating reliability assessments and surfacing regressions, failures, and reliability risks.
- Issue Detection & Tracking: Persistent issue lifecycle management that fingerprints, deduplicates, tracks issues and findings to resolution across recurring review periods. Live Incident Investigation: Real-time investigation of active incidents using LLMs to ingest, correlate, and analyze live observability telemetry alongside codebase context, generating root cause hypotheses and remediation guidance.
- AI-Assisted Reasoning: A conversational, AI-assisted interface for investigating issues, debugging, and reasoning over system and code context.
- Remediation Support: Automated assistance in resolving detected issues, including generating draft remediation actions and code-level Pull Requests for review. Integrations & Notifications: Native integrations with source control, observability, communication, issue tracking, and billing systems (including GitHub, common observability providers, Slack, Microsoft Teams, Linear/Jira, and Stripe) for ingestion, alerting, and workflow synchronization across development, staging, and production environments.

Principal Service Commitments and System Requirements

Beryl designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Beryl makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Beryl has established for the services. The system services are subject to the Security established internally for its services.

System and service commitments are documented and communicated to customers through Service Level Agreements (SLAs), formal customer agreements, and the online description of the service offering available at beryl.so.

Security Commitments

Security commitments include, but are not limited to, the following:

- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal

Components of the System

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.

- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

Infrastructure

The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware that the service organization uses to provide the services.

System/Application	Purpose
AWS ECS Fargate	Serverless container execution orchestration for API and web
AWS RDS PostgreSQL	Managed relational database for primary data storage
AWS ElastiCache Redis	In-memory caching and real-time SSE pub/sub streaming
AWS Elastic Load Balancers	Load balance internal and external traffic
Virtual Private Cloud	Protects the network perimeter and isolates environments
S3 Buckets	Secure storage for chat attachments and static assets

Software

Beryl is responsible for managing the development and operation of the Beryl Software Reliability Platform system including infrastructure components such as servers, databases, and storage systems. The in-scope Beryl infrastructure and software components are shown in the table provided below:

System/Application	Purpose
Amazon Web Services	Primary cloud hosting and infrastructure services including compute (ECS Fargate), database (RDS PostgreSQL), cache (ElastiCache), storage (S3), and networking (VPC).
GitHub	Private repositories for source control, version control, pull request workflows, and automated CI/CD pipelines via GitHub Actions.
Google Cloud Platform	Provides multi-modal (text + image) AI/LLM inference via Google Gemini.
Google Workspace	Internal corporate identity and user authentication via Google Sign-In and One Tap (Google OAuth).
HubSpot	Customer Relationship Management (CRM) platform utilized to manage leads and house customer communication and PII securely.
Langfuse	LLM observability and tracing for monitoring and evaluating AI/LLM inference.

Linear	Issue tracking integration for automated ticket creation from platform findings and webhook based status synchronization.
Microsoft Presidio	Open-source data sanitization tool running internally as a library to actively detect, mask, and redact PII before interactions with AI models.
Postmark	Transactional email delivery for system notifications and customer communications.
Sentry	Real-time error tracking, performance monitoring, and crash reporting for both the frontend and backend applications.
Slack	Internal team communication, real-time reliability and incident notifications, alert routing, and interactive command integrations.
Stripe	Payment processing, self-service subscription management, and webhook-based event processing for billing.
Vanta	Automated compliance monitoring, evidence collection, and policy management for SOC 2.

People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Beryl has a staff of approximately 2 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes:
CEO – Ankesh Khemani

Data

Data as defined by Beryl, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Beryl.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Beryl	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Beryl. Beryl must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Beryl to operate the business. Beryl must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Beryl has policies and procedures in place to properly and securely handle customer data. These policies and procedures are reviewed on at least an annual basis.

Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

Physical Security

Beryl's production servers are maintained by AWS and GCP. The physical and environmental security protections are the responsibility of AWS and GCP. Beryl reviews the attestation reports and performs a risk analysis of AWS and GCP on at least an annual basis.

Logical Access

Beryl provides employees and contractors access to infrastructure via a role based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on an annual basis to ensure least privilege access. Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing

Beryl's policies, and completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in scope systems within 3 days for that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering team for completion and exceptions. If there is an exception, Engineering performs troubleshooting to identify the root cause and will either rerun the backup directly or ensure it runs successfully during the next scheduled job.

Backup infrastructure is maintained in AWS and GCP with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

Beryl maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Beryl internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Beryl utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

Change Management

Beryl maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

Data Communications

Beryl utilizes AWS ECS Fargate to orchestrate its containerized production architecture within an isolated Virtual Private Cloud (VPC). This infrastructure provides robust logical network segmentation and firewall isolation around the application containers, severely restricting ingress traffic exclusively to designated HTTPS web endpoints.
Furthermore, the AWS ECS control plane manages automated container provisioning and recovery gracefully; ensuring failing instances are automatically replaced without operator overhead, preserving SLA targets.
Vulnerabilities are identified through regular vulnerability scans over the system and network over the production environment. Additionally, automated security scanning is built into the CI/CD pipeline, which includes:

- Bandit for Python security static analysis (SAST) on every pull request.
- Gitleaks for automated secrets detection in source code and commit history.
- Dependabot for weekly dependency vulnerability scanning across Python, npm, Docker, and GitHub Actions. pip-audit for Python package vulnerability auditing.

Boundaries of the System

The boundaries of the Beryl Software Reliability Platform are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Beryl Software Reliability Platform.

This report does not include the Cloud Hosting Services provided by AWS and GCP at multiple facilities.

Integrity and Ethical Values

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

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

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

Commitment to Competence

Beryl's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

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

Management's Philosophy and Operating Style

The Beryl management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Beryl can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Beryl to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

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

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

Organizational Structure and Assignment of Authority and Responsibility

Beryl'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.

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

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

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

HR Policies and Practices

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

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

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

Risk Assessment Process

Beryl's risk assessment process identifies and manages risks that could potentially affect Beryl's ability to provide reliable and secure services to our customers. As part of this process, Beryl maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Beryl product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Beryl's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Beryl 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, Beryl's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

Information and Communication Systems

Information and communication are an integral component of Beryl'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.

Beryl uses several information and communication channels internally to share information with management, employees, contractors, and customers. Beryl uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Beryl uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

Monitoring Controls

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

On-going Monitoring

Beryl'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 Beryl's operations help to identify significant variances from expectations regarding internal controls. Upper management evaluates

the facts and circumstances related to any suspected control breakdown. A decision to address 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 Beryl's personnel.

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Changes to the System

During this review period, Beryl repositioned its product, Beryl, as a unified Software Reliability Platform. As part of this repositioning, the system was expanded to add automated reliability testing and monitoring capabilities — including automated validation of customer software via monitored application URLs and endpoints, page crawling, and generated and customer-provided test definitions — alongside the existing live incident investigation and AI-assisted reasoning capabilities. These changes did not alter the underlying security, availability, confidentiality, processing integrity, or privacy commitments made to user entities.

Incidents

No significant incidents have occurred to the services provided to users throughout the audit period.

Criteria Not Applicable to the System

All Common Criteria/Security were applicable to the Beryl's Beryl Software Reliability Platform system.

Subservice Organizations

This report does not include the Cloud Hosting Services provided by AWS and GCP at multiple facilities.

Subservice Description of Services

The Cloud Hosting Services provided by AWS and GCP support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

Beryl'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 the trust services criteria related to Beryl's services to be solely achieved by Beryl control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Beryl

The following subservice organization controls have been implemented by AWS and GCP and included in this report to provide additional assurance that the trust services criteria are met.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Subservice Organization - GCP		
Category	**Criteria**	**Control**
Security	CC 6.4	Data center server floors, network rooms, and security systems are physically isolated from public spaces and/or delivery areas.
		Access to sensitive data center zones requires approval from authorized personnel and is controlled via badge access readers, biometric identification mechanism, and/or physical locks.
		Data center perimeters are defined and secured via physical barriers.
		Access lists to high security areas in data centers are reviewed on a defined basis and inappropriate access is removed in a timely manner.

		Visitors to data center facilities must gain approval from authorized personnel, have their identity verified at the perimeter, and remain with an escort for the duration of the visit.
		Security measures utilized in data centers are assessed annually and the results are reviewed by executive management.
		Data centers are continuously staffed and monitored by security personnel using real time video surveillance and/or alerts generated by security systems.

Beryl management, along with the subservice provider, 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, Beryl performs monitoring of the subservice organization controls, including the following procedures:

- Holding periodic discussions with vendors and subservice organizations.
- Reviewing attestation reports over services provided by vendors and subservice organizations.

Complementary User Entity Controls

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

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

1. User entities are responsible for understanding and complying with their contractual obligations to Beryl
2. User entities are responsible for notifying Beryl 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 Beryl 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 Beryl services.

6. User entities are responsible for providing Beryl with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Beryl of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

Section IV: Description of Criteria, Service Auditor Testing

Section IV: Description of Criteria, Service Auditor Testing

Criteria Common to All Security Principles:

Part A: Trust Criteria and Service Organization Control Activities

CC1.0 – Common Criteria Related to the Control Environment

Criteria	Beryl Control Activity
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	**CA-01** - The company requires contractor agreements to include a code of conduct or reference to the company code of conduct. **CA-02** - The company requires contractors to sign a confidentiality agreement at the time of engagement. **CA-03** - The company requires employees to sign a confidentiality agreement during onboarding. **CA-04** - The company performs background checks on new employees. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-06** - The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CA-07** - The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. **CA-08** - The company's board of directors meets at least annually and maintains formal meeting minutes. **CA-09** - The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. **CA-10** - The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CA-10** - The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. **CA-11** - The company maintains an organizational chart that describes the organizational structure and reporting lines. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-13** - The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.

CC1.0 – Common Criteria Related to the Control Environment

Criteria	Beryl Control Activity
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CA-04** - The company performs background checks on new employees. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-14** - The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CA-01** - The company requires contractor agreements to include a code of conduct or reference to the company code of conduct. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-06** - The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

CC2.0 – Common Criteria Related to Communication and Information

Criteria	Beryl Control Activity
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-17** - The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. **CA-18** - The company communicates system changes to authorized internal users. **CA-19** - The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. **CA-20** - The company provides a description of its products and services to internal and external users. **CA-21** - The company's information security policies and procedures are documented and reviewed at least annually.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-13** - The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. **CA-14** - The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. **CA-18** - The company communicates system changes to authorized internal users. **CA-19** - The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. **CA-20** - The company provides a description of its products and services to internal and external users. **CA-21** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.

CC2.0 – Common Criteria Related to Communication and Information

Criteria	Beryl Control Activity
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CA-04** - The company performs background checks on new employees. **CA-23** - The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS). **CA-24** - The company provides guidelines and technical support resources relating to system operations to customers. **CA-25** - The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. **CA-26** - The company notifies customers of critical system changes that may affect their processing. **CA-27** - The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

CC3.0 – Common Criteria Related to Risk Assessment

Criteria	Beryl Control Activity
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-29** - The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually. **CA-32** - The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-34** - The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

CC4.0 – Common Criteria Related to Monitoring Activities

Criteria	Beryl Control Activity
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.

CC5.0 – Common Criteria Related to Control Activities

Criteria	Beryl Control Activity
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CA-21** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CA-21** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.

CC5.0 – Common Criteria Related to Control Activities

Criteria	Beryl Control Activity
CC5.3 - **COSO Principle 12:** The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-21** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-29** - The company specifies its objectives to enable the identification and assessment of risk related to the objectives. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-38** - The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-40** - The company's data backup policy documents requirements for backup and recovery of customer data.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

Criteria	Beryl Control Activity
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.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-41** - The company's datastores housing sensitive customer data are encrypted at rest. **CA-42** - The company restricts privileged access to encryption keys to authorized users with a business need. **CA-43** - The company restricts privileged access to the firewall to authorized users with a business need. **CA-44** - The company's network is segmented to prevent unauthorized access to customer data. **CA-45** - The company requires passwords for in-scope system components to be configured according to the company's policy. **CA-46** - The company restricts privileged access to the application to authorized users with a business need. **CA-47** - The company restricts privileged access to databases to authorized users with a business need. **CA-48** - The company maintains a formal inventory of production system assets. **CA-49** - The company restricts privileged access to the production network to authorized users with a business need. **CA-50** - The company restricts privileged access to the operating system to authorized users with a business need. **CA-51** - The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-53** - The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. **CA-54** - The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. **CA-55** - The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. **CA-56** - The company restricts access to migrate changes to production to authorized personnel.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

Criteria	Beryl Control Activity
	CA-57 - The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. **CA-58** - The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.
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.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-53** - The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. **CA-59** - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. **CA-60** - The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
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.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-53** - The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. **CA-59** - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. **CA-60** - The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.

CC6.0 – Common Criteria Related to Logical and Physical Access Controls

Criteria	Beryl Control Activity
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.	**CA-38** - The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. **CA-60** - The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs. **CA-62** - The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. **CA-63** - The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CA-53** - The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys. **CA-54** - The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. **CA-55** - The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. **CA-65** - The company uses firewalls and configures them to prevent unauthorized access. **CA-66** - The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-68** - The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. **CA-69** - The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.
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.	**CA-66** - The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. **CA-70** - The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. **CA-71** - The company encrypts portable and removable media devices when used.
CC6.8 - The entity implements controls to prevent or detect and act	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to

Criteria	Beryl Control Activity
upon the introduction of unauthorized or malicious software to meet the entity's objectives.	remediation. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-73** - The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

CC7.0 – Common Criteria Related to Systems Operations

Criteria	Beryl Control Activity
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.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-34** - The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. **CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-74** - The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
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.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-17** - The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-68** - The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. **CA-74** - The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring. **CA-75** - An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

CC7.0 – Common Criteria Related to Systems Operations

Criteria	Beryl Control Activity
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.	**CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-76** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
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.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-76** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. **CA-77** - The company tests their incident response plan at least annually.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-32** - The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. **CA-76** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. **CA-77** - The company tests their incident response plan at least annually.

CC8.0 – Common Criteria Related to Change Management

Criteria	Beryl Control Activity
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.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-56** - The company restricts access to migrate changes to production to authorized personnel. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-69** - The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

CC9.0 – Common Criteria Related to Risk Mitigation

Criteria	Beryl Control Activity
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-79** - The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions. **CA-80** - The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**CA-27** - The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.

Part B: Testing of Controls and Results

Control Activity	Tests Performed	Test Results
CA-01 - The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Code of Conduct to determine that the company required contractor agreements to include a code of conduct or reference to the company code of conduct. Inspected the contractor agreement for a sample of contractors to determine that the company required contractors agree to the code of conduct.	No exceptions noted.
CA-02 - The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the signed Code of Conduct Policy to determine that the company required contractors to sign a confidentiality agreement at the time of engagement. Inspected the contractor agreement for a sample of contractors to determine that the company required contractors to sign a confidentiality agreement at the time of engagement.	No exceptions noted.
CA-03 - The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed Code of Conduct Policy to determine that the company required employees to sign a confidentiality agreement at the time of engagement. Inspected the employee agreement to determine that the company required employees to sign a confidentiality agreement at the time of engagement. Inspected the signed employee agreement for a sample of employees to determine that employees signed a confidentiality agreement at the time of engagement.	No exceptions noted.
CA-04 - The company performs background checks on new employees.	Inspected the signed Code of Conduct Policy to determine that the company required background checks on new employees. Inspected the completed background check for a sample of new hires to determine that the company required background checks on new employees.	Testing of this control activity disclosed that there were no new hires during the review period.
CA-05 - The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the signed Code of Conduct Policy to determine that the company managers were required to complete performance evaluations for direct reports at least annually. Inspected the completed performance reviews for a sample of employees to determine company managers completed performance evaluations for direct reports at least annually.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-06 - The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the Code of Conduct to determine that the company required employees to acknowledge a code of conduct at the time of hire. Employees who violated the code of conduct were subject to disciplinary actions in accordance with the disciplinary policy. Inspected the signed Code of Conduct Policy to determine that the company required employees to acknowledge a code of conduct at the time of hire. Employees who violated the code of conduct were subject to disciplinary actions in accordance with the disciplinary policy. Inspected the signed Code of Conduct Policy for a sample of employees to determine employees agreed to the policy. Inspected the signed Human Resource Security Policy for a sample of employees to determine that employees agreed to the policy.	No exceptions noted.
CA-07 - The company's board members or a relevant subcommittee have sufficient expertise to oversee management's ability to design, implement and operate information security controls.	Inspected the board charter to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement and operate information security controls. Inspected the backgrounds and experiences for a sample of board members to determine that the company's board members had sufficient expertise to oversee management's ability to design, implement and operate information security controls.	No exceptions noted.
CA-08 - The company's board of directors or a relevant subcommittee meets at least annually and maintains formal meeting minutes.	Inspected the board charter to determine that the company's board members were required to meet at least annually and maintained formal meeting minutes. Inspected the board meeting minutes for a sample of board meetings to determine that the company's board of directors met at least annually and maintained formal meeting minutes.	No exceptions noted.
CA-09 - The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the board meeting minutes for a sample of board meetings to determine that the company's board of directors or a relevant subcommittee was briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	No exceptions noted.
CA-10 - The company's board of directors or a relevant subcommittee has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the board charter to determine that the company had documented the oversight responsibilities for internal control. Inspected the organizational chart to determine that the company had documented the oversight responsibilities for internal control.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-11 - The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company documented the organizational structure and reporting lines. Inspected the organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines. Inspected the board charter to determine that the company had documented the outlines of the board and its oversight responsibilities for internal control.	No exceptions noted.
CA-12 - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy. Inspected the job description for a sample of roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CA-13 - The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management had established defined roles and responsibilities to oversee the design and implementation of information security controls. Inspected the signed Information Security Roles and Responsibilities Policy for a sample of employees to determine that employees agreed to the policy.	No exceptions noted.
CA-14 - The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the signed Code of Conduct Policy to determine that employees were required to complete security awareness training timely after hire and on a regular cadence thereafter. Inspected the information security training program to determine that the company required current employees to complete security awareness training at least annually. Inspected the completed information security training for a sample of employees to determine that the company required current employees to complete security awareness training at least annually.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-15 - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the job description to determine that the company required control self-assessments at least annually to gain assurance that controls were in place and operating effectively. Corrective actions were required based on relevant findings. Inspected the completed risk assessment to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating as expected. Corrective actions were taken based on relevant findings or in the event of an identified issue. Inspected the monitoring tool configurations and an example alert to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating as expected. Corrective actions were taken based on relevant findings or in the event of an identified issue.	No exceptions noted.
CA-16 - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operation Security Policy to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the vulnerability scanning configurations to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation. Inspected the remediated vulnerability tickets for a sample of vulnerabilities found in critical systems to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems, and that critical and high vulnerabilities were tracked to remediation.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-17 - The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the Operation Security Policy to determine that the company utilized a log management tool to identify events that may have potential impact on the company's ability to achieve its security objectives Inspected the client's GCP instance to determine access to logging configurations is restricted to authorized users. Inspected the client's GCP instance to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives. Inspected the CloudTrail configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives. Inspected the AWS user access listing and permissions to determine that access to logging configurations is restricted to authorized users. Inspected the AWS log configurations to determine that the company utilized a log management tool to identify and track events that may have potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CA-18 - The company communicates system changes to authorized internal users.	Inspected the update instructions to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CA-19 - The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the job description to determine that the company had established a formalized whistle blower policy, and an anonymous communication channel was in place for users to report potential issues or fraud concerns. Inspected the anonymous reporting channel to determine that the company had established a formalized whistle blower policy, and an anonymous communication channel was in place for users to report potential issues or fraud concerns.	No exceptions noted.
CA-20 - The company provides a description of its products and services to internal and external users.	Inspected the product information on the company website to determine that the company provided a description of its products and services to internal and external users. Inspected the network diagram to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CA-21 - The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the relevant information security policies to determine that the company's information security policies and procedures were documented and reviewed at least annually. Inspected the signed company policies for a sample of employees to determine that employees agreed to the policies.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-22 - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the signed company policies to determine that the company had security and privacy incident response policies in place. Inspected the signed Incident Response Policy for a sample of employees to determine employees agreed to the policy.	No exceptions noted.
CA-23 - The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the master service agreement to determine that the company's security commitments were communicated to customers in a MSA or TOS. Inspected the terms of service to determine that the company's security commitments were communicated to customers in a MSA or TOS.	No exceptions noted.
CA-24 - The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's support page to determine that the company provided guidelines and technical support resources relating to system operations to customers. Inspected the release notes to determine that the company provided guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CA-25 - The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company has policies in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. Inspected the company's support page to determine that the company has a system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CA-26 - The company notifies customers of critical system changes that may affect their processing.	Inspected the Operation Security Policy to determine that the company had policies and processes on how to notify customers of critical system changes that may affect their processing. Inspected the application status webpage to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-27 - The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Privacy Policy on the company website to determine that the company publicly disclosed its confidentiality and privacy commitments. Inspected the list of vendors to determine that the company had written agreements in place with vendors and related third-parties. These agreements included confidentiality and privacy commitments applicable to that entity. Inspected the vendor agreement for a sample of critical vendors to determine that the company had written agreements in place with vendors and related third-parties. These agreements included confidentiality and privacy commitments applicable to that entity. Inspected a sample of third-party vendors to determine the company assigned risks to vendors.	No exceptions noted.
CA-28 - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies.	Inspected the Risk Management Policy to determine that the company had a documented risk management program in place, including guidance on the identification of potential threats, rating the significance of risks associated with identified threats, and mitigation strategies for those risks. Inspected the signed Risk Management Policy for a sample of employees to determine that employees agreed to the policy.	No exceptions noted.
CA-29 - The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives. Inspected the completed risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives on an annual basis.	No exceptions noted.
CA-30 - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the Risk Management Policy to determine that the company's risk assessment was performed annually. Threats and changes to services commitments were identified and the risk were formally assessed. The risk assessment included a consideration of the potential for fraud. Inspected the completed risk assessment to determine that the company's risk assessment was performed annually. Threats and changes to services commitments were identified and the risk were formally assessed. The risk assessment included a consideration of the potential for fraud.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-31 - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the list of vendors to determine that the company tracks and inventories their third-party vendors. Inspected the company's policies to determine that the company had a vendor management program in place which included third-party inventory, security and privacy requirements, and review of vendors annually. Inspected the attestation report and security assessments for a sample of critical vendors to determine that the company had a vendor management program in place and included the relevant components. Inspected a sample of third-party vendors to determine the company assigned risks to vendors.	No exceptions noted.
CA-32 - The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity/Disaster Recovery Policy to determine that the company had a documented BC/DR plan. Inspected the signed Business Continuity/Disaster Recovery policy for an example employee to determine that the company had a documented BC/DR plan. Inspected the completed tabletop exercise to determine that the company had a documented BC/DR plan and had tested it at least annually.	No exceptions noted.
CA-34 - The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operation Security Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment. Inspected the deployment system configurations and an example change to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-35 - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements.	Inspected the Operations Security Policy to determine that the company had a formal system development life cycle methodology in place to govern the development, acquisition, implementation, changes (including emergencies), and maintenance of information systems and related technology requirements. Inspected the signed Operations Security Policy for a sample of employees to determine that the company had a formal system development life cycle methodology in place to govern the development, acquisition, implementation, changes (including emergencies), and maintenance of information systems and related technology requirements. Inspected the Secure Development Policy to determine that the company had a formal system development life cycle methodology in place to govern the development, acquisition, implementation, changes (including emergencies), and maintenance of information systems and related technology requirements. Inspected the signed Secure Development Policy for a sample of employees to determine that the company had a formal system development life cycle methodology in place to govern the development, acquisition, implementation, changes (including emergencies), and maintenance of information systems and related technology requirements.	No exceptions noted.
CA-36 - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.	Inspected the access policies of the company to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the signed access policies for a sample of employees to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. Inspected the signed Access Control Policy for a sample of current employees to determine that the company's access control policy documented the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.	Testing of this control activity disclosed that there were no access requests during the review period.
CA-38 - The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the company's data management policies to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. Inspected the signed data management policies for a sample of employees to determine that employees agree to the company's data management practices.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-39 - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected the Operation Security Policy to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. Inspected the pull requests for a sample of changes to determine that the changes followed the defined change management process. Inspected the client's version control tool to determine that the configurations followed the defined change management process. Inspected the deployment system configurations and an example change to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. Inspected the change ticket for a sample of application changes to determine that the changes followed the defined change management process.	No exceptions noted.
CA-40 - The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the company policies to determine that the company's data backup policy documents requirements for backup and recovery of customer data. Inspected the signed company policies for a sample of employees to determine that the company's data backup policy documents requirements for backup and recovery of customer data. Inspected the completed tabletop exercise to determine that the company's data backup policy documents requirements for backup and recovery of customer data.	No exceptions noted.
CA-41 - The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the Cryptography Policy to determine that the company's datastores housing sensitive customer data were encrypted at rest. Inspected the client's GCP instance to determine that the configurations for company datastores followed the defined encryption requirements for safeguarding customer data at rest. Inspected the AWS account encryption configurations to determine that the configurations for company datastores followed the defined encryption requirements for safeguarding customer data at rest. Inspected the encryption configurations to determine that the configurations for company datastores followed the defined encryption requirements for safeguarding customer data at rest.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-42 - The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Cryptography Policy to determine that the company restricts privileged access to encryption keys to authorized users with a business need. Inspected the company's user listings to determine that the company restricts privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
CA-43 - The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Asset Management Policy to determine that the company restricted privileged access to the firewall to authorized users with a business need. Inspected the client's AWS account to determine that the company firewall rulesets restricted privileged access to the firewall to authorized users with a business need. Inspected the client's AWS account to determine that the company port configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the client's AWS account to determine that the company SSH configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the EC2 port configurations to determine that the company port configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the user access listing and SSH keys provisioned to determine that the company SSH configurations restricted privileged access to the firewall to authorized users with a business need. Inspected the client's AWS firewall rule set to determine that the company firewall rulesets restricted privileged access to the firewall to authorized users with a business need. Inspected the SSH configurations to determine that the company SSH configurations restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CA-44 - The company's network is segmented to prevent unauthorized access to customer data.	Inspected the Information Security Policy to determine that the company's network was segmented from the public network to prevent unauthorized access to customer data. Inspected the network diagram to determine that the company's network was segmented from the public network to prevent unauthorized access to customer data.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-45 - The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the Access Control Policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy. Inspected the signed Access Control Policy for a sample of employees to determine that employees agreed to the company's password requirements. Inspected the password configurations for in-scope systems to determine that they were in accordance with the company's policy. Observed that password managers were in use on user endpoints to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CA-46 - The company restricts privileged access to the application to authorized users with a business need.	Inspected the Access Control Policy to determine that the company restricted privileged access to the application to authorized users with a business need. Inspected the administrator user listings to critical applications to determine that the company restricted privileged access to the application to authorized users with a business need.	No exceptions noted.
CA-47 - The company restricts privileged access to databases to authorized users with a business need.	Inspected the Access Control Policy to determine that the company restricted privileged access to databases to authorized users with a business need. Inspected the user listing of database administrator to determine that the company restricted privileged access to databases to authorized users with a business need.	No exceptions noted.
CA-48 - The company maintains a formal inventory of production system assets.	Inspected the Asset Management Policy to determine that the company maintained a formal inventory of production system assets. Inspected the inventory listing to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CA-49 - The company restricts privileged access to the production network to authorized users with a business need.	Inspected the Access Control Policy to determine that the company required authentication to the production network to authorized users with a business need. Inspected the network administrator user listing to determine that the company restricted privileged access to the production network to authorized users with a business need.	No exceptions noted.
CA-50 - The company restricts privileged access to the operating system to authorized users with a business need.	Inspected the Access Control Policy to determine that the company restricted privileged access to the operating system to authorized users with a business need. Inspected the network user listing to determine that the company restricted privileged access to the operating system to authorized users with a business need.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-51 - The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as MFA or unique SSH key.	Inspected the Access Control Policy to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key. Inspected the database user listing and password configurations to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms.	No exceptions noted.
CA-52 - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the Access Control Policy to determine that the company ensured that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned. Inspected the signed Access Control Policy for a sample of current employees to determine that the company ensured that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
CA-53 - The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the encryption configurations and SSL certificate to determine that the company required authentication to the production network required unique usernames and passwords or authorized SSH keys. Inspected the SSH configurations to determine that the company required authentication to the production network required unique usernames and passwords or authorized SSH keys. Inspected the password configurations to determine that the company required authentication to the production network required unique usernames and passwords or authorized SSH keys.	No exceptions noted.
CA-54 - The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the Access Control Policy to determine that the company established requirements that production systems can only be remotely accessed by authorized employees via an approved encrypted connection. Inspected the encryption configurations and SSL certificate to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CA-55 - The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the Access Control Policy to determine that the company requires production systems to only be remotely accessed by authorized employees possessing a valid MFA method. Inspected the company's user listings, system and password configurations to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-56 - The company restricts access to migrate changes to production to authorized personnel.	Inspected the Operation Security Policy to determine that the company restricted access to migrate changes to production to authorized personnel. Inspected the Secure Development Policy to determine that the company restricted access to migrate changes to production to authorized personnel. Inspected the change tickets for a sample of application changes to determine that the company restricted access to migrate changes to production to authorized personnel. Inspected the version control configurations to determine that the company restricted access to migrate changes to production to authorized personnel. Inspected the pull requests for a sample of changes to determine that the company restricted access to migrate changes to production to authorized personnel. Inspected the client's version control tool to determine that the tool was configured to restrict access to migrate changes to production to authorized personnel.	No exceptions noted.
CA-57 - The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the Data Management Policy to determine that the company had a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. Inspected the signed Data Management Policy for a sample of employees to determine that employees agreed to the policy.	No exceptions noted.
CA-58 - The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company required authentication to systems and applications to use unique username and password or authorized SSH keys. Inspected the application administrator user listing to determine that the company required authentication to systems and applications to use unique username and password or authorized SSH keys.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-59 - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the Access Control Policy to determine that the company conducted access reviews at least quarterly for the in-scope system components to help ensure that access was restricted appropriately. Required changes are tracked to completion. Inspected the client's cloud provider configurations to determine that the company monitors and remediates identified issues, tracking changes to completion. Inspected the completed user access reviews for a sample of production access reviews to determine that the company conducted reviews at least quarterly for the in-scope system components to ensure that access was restricted appropriately. Required changes are tracked to completion. Inspected the client's user listings for in-scope system components to ensure all accounts are associated with users. Inspected the client's identity provider configurations to determine that the company monitors and remediates identified issues, tracking changes to completion.	No exceptions noted.
CA-60 - The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company termination checklists require access to be revoked for terminated employees within SLAs. Inspected the Employee Termination Policy to determine that the company termination checklists require access to be revoked for terminated employees within SLAs. Inspected the access reviews for selected periods to determine that terminated user accounts did not have access to in-scope systems. Inspected the company user listings and a sample of terminated users to determine that the company completed termination checklists for terminated employees and was within defined SLAs.	No exceptions noted.
CA-62 - The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the Asset Management Policy to determine that the company had electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed. Inspected the signed Asset Management Policy for a sample of employees to determine that employees agreed to the company policy. Inspected the disposal listing for a sample of disposal requests to determine that the company had electronic media containing confidential information was purged or destroyed in accordance with best practices, and certificates of destruction were issued for each device destroyed.	Testing of this control activity disclosed that there were no media devices destroyed or purged during the review period.

Control Activity	Tests Performed	Test Results
CA-63 - The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Management Policy to determine that the company requires the purge or removal of customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service. Inspected the customer deletion requests from a sample of customers to determine that the company purged or removed customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Testing of this control activity disclosed that there were no customer data deletion requests during the review period.
CA-65 - The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall configurations to determine that the company uses firewalls and configures them to prevent unauthorized access. Inspected the company's SSH configurations to determine that the company uses firewalls and configures them to prevent unauthorized access.	No exceptions noted.
CA-66 - The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Cryptography Policy to determine that the company had a documented process around secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Inspected the client's cloud load balancer configurations to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. Inspected the SSL certificates to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CA-67 - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the Operation Security Policy to determine that the company required infrastructure supporting the service patch as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers and supporting the service were hardened against security threats. Inspected the vulnerability scanning configurations to determine that the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats. Inspected a sample of remediated vulnerabilities to determine that the company had infrastructure supporting the service patching as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-68 - The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operation Security Policy to determine that the company requires continuous monitoring of the company's network and early detection of potential security breaches. Inspected the CloudTrail configurations to determine that the company provides continuous monitoring of the company's network and early detection of potential security breaches. Inspected the MDM tool dashboard to determine that the company provides continuous monitoring of the company's network and early detection of potential security breaches. Inspected the client's AWS configurations to determine that the company provides continuous monitoring of the company's network and early detection of potential security breaches. Inspected the client's security configurations to determine that the company provides continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CA-69 - The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operation Security Policy to determine that the company requires network and system hardening standards documented, based on industry best practices, and reviewed at least annually. Inspected the client's security settings and configurations to determine that the company's network and system hardening standards were documented, based on industry best practices, and reviewed at least annually. Inspected the client's annual firewall review to determine that the firewall configurations meet the company's hardening standards.	No exceptions noted.
CA-70 - The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the job description to determine that the company had requirements around a MDM system in place to centrally manage mobile devices supporting the service. Inspected the client's MDM tool configurations to determine that the company had a MDM system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CA-71 - The company encrypts portable and removable media devices when used.	Inspected the Cryptography Policy to determine that the company requires encryption of portable and removable media devices when used. Inspected the endpoint encryption configurations for a sample of endpoint devices to determine that the company encrypted portable and removable media devices when used. Inspected the MDM tool for a sample of endpoint devices to determine that the company encrypted portable and removable media devices when used.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-73 - The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the job description to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems. Inspected the MDM tool dashboard for a sample of endpoint devices to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
CA-74 - The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's policies to determine that the formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring. Inspected the signed policies for a sample of employees to determine that employees agreed to the company's formal policies for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CA-75 - An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Operation Security Policy to determine an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	No exceptions noted.
CA-76 - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the signed company policies to determine that the company required security and privacy incidents to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. Inspected the signed policies for a sample of employees to determine that employees agreed to the company incident response policies Inspected the resolved security incidents for a sample of security incidents to determine that the company required security and privacy incidents to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Testing of this control activity disclosed that there were no security incidents noted during the review period.
CA-77 - The company tests their incident response plan at least annually.	Inspected the signed company policies to determine that the company required testing their incident response plan at least annually. Inspected the Incident Response Plan to determine that the company tested their incident response plan at least annually.	No exceptions noted.

Control Activity	Tests Performed	Test Results
CA-79 - The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the Operation Security Policy to determine that the company considered cybersecurity insurance to mitigate the financial impact of business disruptions. Inspected the risk assessment to determine that the company considered cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CA-80 - The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity/Disaster Recovery policies to determine that the company had BC/DR plans in place that outlined communication plans in order to maintain information security continuity in the event of the unavailability of key personnel. Inspected the signed Business Continuity/Disaster Recovery policies to determine that employees agreed to the policies.	No exceptions noted.