

Vibemonitor, Inc.

System and Organization Controls (SOC) 2 Report

Software Reliability Platform

As of April 1, 2026

Advantage PARTNERS

Table of Contents

SECTION I: INDEPENDENT SERVICE AUDITOR'S REPORT 5
SECTION II: MANAGEMENT'S ASSERTION 10
SECTION III: DESCRIPTION OF THE SYSTEM 13
SECTION IV: DESCRIPTION OF CRITERIA, SERVICE AUDITOR TESTING 31

Executive Summary

Vibemonitor, Inc. - Software Reliability Platform

Scope	Software Reliability Platform
Period of Examination	As of April 1, 2026
Subservice Providers	Amazon Web Service (AWS) and 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 28**

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. ("Vibemonitor" or the "Service Organization") of its Software Reliability Platform as of April 1, 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 of controls stated in the description as of April 1, 2026, to provide reasonable assurance that Vibemonitor'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)*.

Vibemonitor uses a subservice organization for cloud hosting services listed in **Section III**. The description indicates that complementary subservice organization controls that are suitably designed are necessary, along with controls at Vibemonitor, to achieve Vibemonitor's service commitments and system requirements based on the applicable trust services criteria. The description presents Vibemonitor's controls, the applicable trust services criteria, and the complementary subservice organization controls assumed in the design of Vibemonitor's controls. The description does not extend to the controls of the user entity.

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

Our responsibility is to express an opinion on the description and on the suitability of the design 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 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 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;
- 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.

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.

The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description, and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description fairly presents the Software Reliability Platform systems of Vibemonitor that was designed and implemented as of April 1, 2026 in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of April 1, 2026, to provide reasonable assurance that Vibemonitor‘s service commitments and system requirements would be achieved based on the applicable trust services criteria, if the controls operated effectively as of that date.

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 Vibemonitor, user entities of the in-scope services for Vibemonitor's Software Reliability Platform systems as of April 1, 2026, business partners of Vibemonitor subject to risks arising from interactions with Software Reliability Platform system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Service Organization.
- How the Service Organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary 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

May 28, 2026

Section II:
Management's Assertion

Section II: Management's Assertion

Vibemonitor's Assertion

We have prepared the accompanying description of the Software Reliability Platform system in **Section III** of Vibemonitor ("Service Organization") as of April 1, 2026 (the "as-of date"), 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 Vibemonitor system that may be useful when assessing the risks that arise from interactions with Vibemonitor system, particularly information about system controls that Vibemonitor 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 Vibemonitor, to achieve the service commitments and system requirements based on the applicable trust service criteria. The description presents Vibemonitor's controls, the applicable trust service criteria, and the complementary subservice organization controls assumed in the design of Vibemonitor'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 Vibemonitor, to achieve Vibemonitor's service commitments and system requirements based on the applicable trust services criteria. The Description presents Vibemonitor's controls; the applicable trust services criteria; and the complementary user entity controls assumed in the design of Vibemonitor'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 Vibemonitor's system that was designed and implemented as of April 1, 2026 in accordance with the description criteria.

b. The controls stated in the description were suitably designed as of April 1, 2026 to provide reasonable assurance that Vibemonitor's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of April 1, 2026 and if the subservice

organization applied the complementary controls assumed in the design of Vibemonitor controls as of April 1, 2026.

Section III:
Description of the System

Section III: Description of the System

Company Background

Vibemonitor, Inc. provides an AI-powered application performance monitoring and observability platform designed to assist engineering teams in monitoring and maintaining software reliability. 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

Vibemonitor is an AI-powered Software as a Service (SaaS) service Software Reliability Platform. The system is designed to help software engineering teams audit service health risks, detect telemetry gaps, actively investigate live incidents with Agentic RCA, and track actions to fix them.

- **Service Health Reviews:** Automated, recurring audits of service health using code fact extraction, deterministic rules, and LLM-powered verification/enrichment to produce health scores and ranked findings.
- **Service Health Issue Tracking:** Persistent issue lifecycle management that fingerprints, deduplicates, and tracks resolution status across review periods, featuring search and pagination capabilities.
- **Agentic Root Cause Analysis (RCA):** Automated, real-time investigation of active incidents using LLMs to ingest, correlate, and analyze live observability telemetry alongside codebase context, instantly generating root cause hypotheses and automated remediation plans.
- **AI Chat Interface:** An intelligent conversational interface with SSE streaming, file uploads, and session management for investigating issues and debugging.
- **Status Page:** Public status page powered by Instatus (status.beryl.so) for real-time communication of system availability and incidents.
- **GitHub Integration:** Native integration for codebase synchronization, code parsing, deployment tracking, automated issue creation, and automated generation of remediation Pull Requests (Draft state) for detected code-level vulnerabilities and gaps.
- **Observability Integrations:** Ingestion and correlation of metrics, logs, and application performance data from Datadog, Grafana, New Relic, AWS CloudWatch, Google Cloud Platform (GCP Logging), and Azure Monitor.
- **Slack and Microsoft Teams Integration:** Real-time health review notifications, alert routing, and interactive management via Slack and Microsoft Teams.
- **Linear / Jira Integration:** Native issue tracking integration for automated ticket creation and webhook-based status synchronization.

- **Multi-Environment Support:** Monitoring across development, staging, and production environments with configurable alerting thresholds.
- **Billing and Subscription Management:** Self-service subscription management via Stripe.

Principal Service Commitments and System Requirements

Vibemonitor designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Vibemonitor makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Vibemonitor has established for the services. The system services are subject to the Security, Confidentiality, Availability, Processing integrity, and Privacy commitments 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 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, and penetration tests 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.
- Up time availability of production systems.

Components of the System

The System description is comprised of the following components:

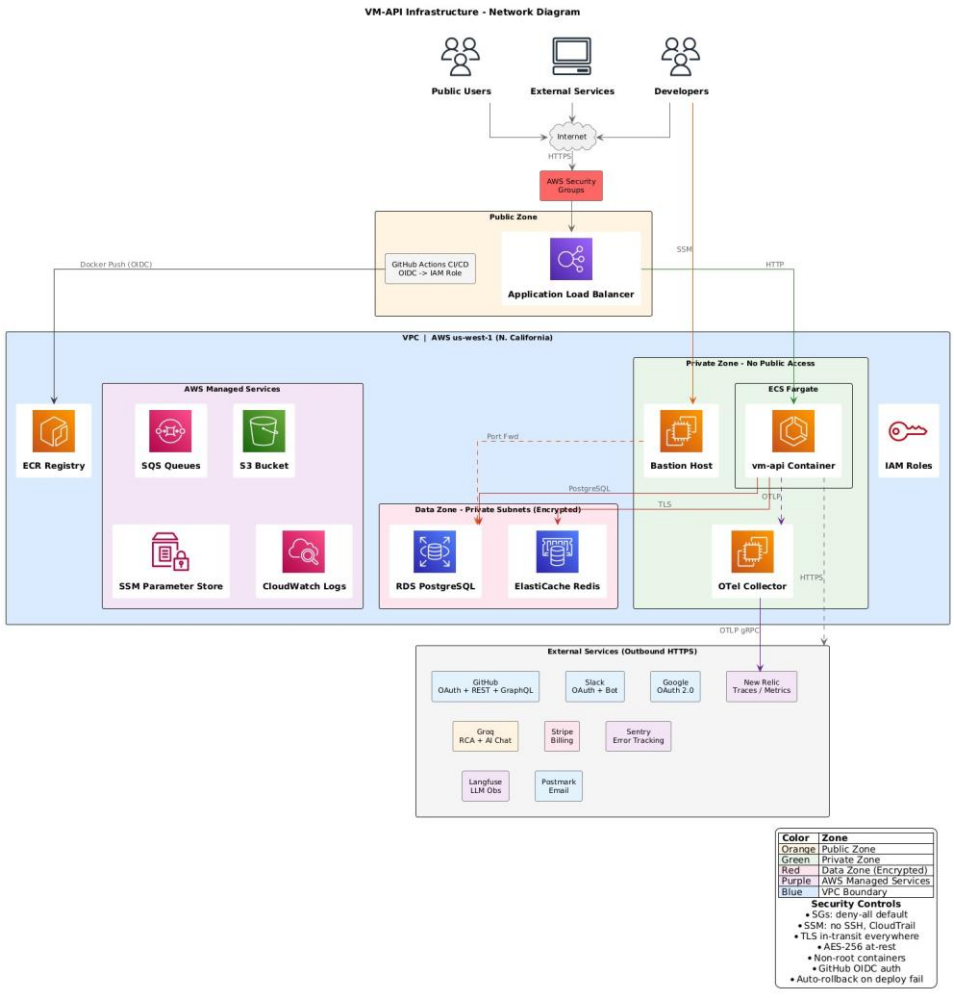
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of

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

Vibemonitor maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner. To outline the topology of its network, the organization maintains the following network diagram.



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

Software

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

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

Linear	SaaS	Issue tracking integration for automated ticket creation from health review findings and webhook-based status synchronization.
Microsoft Presidio	Internal Library	Open-source data sanitization tool running internally as a library to actively detect, mask, and redact PII before interactions with AI models.
OpenTelemetry Collector	Internal Container	Gateway that batches and forwards the application's internal traces, metrics, and logs to observability systems via OTLP.
Postmark		
Sentry	SaaS	Real-time error tracking, performance monitoring, and crash reporting for both the frontend and backend applications.
Slack	SaaS	Internal team communication, real-time health review notifications, alert routing, and interactive command integrations.
Stripe	SaaS	Payment processing, self-service subscription management, and webhook-based event processing for billing.
Vanta	SaaS	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.

Vibemonitor has a staff of 5 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. As an early-stage startup operating under a single-director governance model, this includes: CEO - Ankesh Khemani.
- **Operations:** Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

- **Information Technology:** Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.
- **Product Development:** Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality. This team comprises core engineering (Tanay, Tarpita, Tushar, Akshat) and design (Priya) personnel.
- **Sales & Marketing:** Responsible for go-to-market operations, managing prospective customer communications, and maintaining lead data within the CRM. This function is managed by Ankesh and Tanay.

Data

Data, as defined by Vibemonitor, 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 Vibemonitor.

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

	possible levels of integrity, confidentiality, and restricted availability for this information.	• 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, Vibemonitor 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

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

Logical Access

Vibemonitor 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 a quarterly 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 Vibemonitor's policies and completing security training. These steps must be completed within 14 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, the Engineering Team will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure natively utilized by the RDS PostgreSQL database is maintained entirely within AWS, with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

Vibemonitor 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.

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

Vibemonitor 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

Vibemonitor 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

Vibemonitor 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, as well as penetration tests 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 Software Reliability Platform system 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 Software Reliability Platform system.

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 Vibemonitor's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Vibemonitor'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

Vibemonitor'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 Vibemonitor 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 Vibemonitor 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 Vibemonitor 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

Vibemonitor'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.

Vibemonitor'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

Vibemonitor'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. Vibemonitor'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

Vibemonitor’s risk assessment process identifies and manages risks that could potentially affect Vibemonitor’s ability to provide reliable and secure services to our customers. As part of this process, Vibemonitor 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 Vibemonitor 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 Vibemonitor’s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Vibemonitor 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, Vibemonitor’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 Vibemonitor'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.

Vibemonitor uses several information and communication channels internally to share information with management, employees, contractors, and customers. Vibemonitor 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, Vibemonitor 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. Vibemonitor's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-going Monitoring

Vibemonitor'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 Vibemonitor'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 for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Vibemonitor'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

As of the date of this report, major architectural and infrastructural modifications were implemented to improve reliability and security:

- Migrated Vibemonitor's internal application performance monitoring from New Relic to Sentry.
- Migrated the primary relational database datastore from Supabase to AWS RDS PostgreSQL to ensure robust connection pooling and uptime stability.
- Transitioned organizational workflow to an in-office model to optimize operational communication and oversight.

Incidents

No significant incidents have occurred to the services provided to users as of the date of this report.

Criteria Not Applicable to the System

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

Subservice Organizations

This report does not include the Cloud Hosting Services provided AWS and GCPat 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

Vibemonitor’s services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Vibemonitor’s services to be solely achieved by Vibemonitor control procedures. Accordingly, subservice organizations, in conjunction with the services,

should establish their own internal controls or procedures to complement those of Vibemonitor.

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.

Vibemonitor 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, Vibemonitor performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports.
- Holding periodic discussions with vendors and subservice organization(s).
- Testing controls performed by vendors and subservice organization(s).
- Reviewing attestation reports over services provided by vendors and subservice organization(s).
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization.

Complementary User Entity Controls

Vibemonitor'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 Vibemonitor's services to be solely achieved by Vibemonitor control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Vibemonitor'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 Vibemonitor.
2. User entities are responsible for notifying Vibemonitor 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 Vibemonitor 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 Vibemonitor services.
6. User entities are responsible for providing Vibemonitor with a list of approvers for security and system configuration changes for data transmission.

7. User entities are responsible for immediately notifying Vibemonitor 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	Vibemonitor 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.

CC1.0 – Common Criteria Related to the Control Environment

Criteria	Vibemonitor Control Activity
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.
CC1.4 - 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 fourteen 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	Vibemonitor 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 fourteen 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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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 Identity-Based Secure Tunneling Engine 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 Identity-Based Secure Tunneling Engine 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	Vibemonitor 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 Identity-Based Secure Tunneling Engine 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 Identity-Based Secure Tunneling Engine 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 Identity-Based Secure Tunneling Engine 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	Vibemonitor 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 Identity-Based Secure Tunneling Engine 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.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

Criteria	Vibemonitor Control Activity
or malicious software to meet the entity's objectives.	**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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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	Vibemonitor 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.