Sardine

SYSTEM AND ORGANIZATION CONTROLS (SOC) 2® TYPE 2 REPORT ON MANAGEMENT'S DESCRIPTION OF ITS

Sardine Financial Crime and Fraud Prevention, Payments, and Consortium Services

And on the Suitability of Design and Operating Effectiveness of Its Controls Relevant to Trust Services Criteria for Security, Availability, and Confidentiality

For the period June 1, 2025 to May 31, 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

This report is confidential, and its use is limited to SardineAI Corp. and its user organizations and the independent auditors of its user organizations. Unauthorized use of this report in whole or in part is strictly prohibited.

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report 1

Scope 1

Service Organization's Responsibilities 1

Service Auditors' Responsibilities 2

Inherent Limitations 3

Description of Tests of Controls 3

Opinion 3

Restricted Use 4

2. Assertion of Sardine Management 5

3. Description of Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services 7

Company Background 7

Services Provided 7

Principal Service Commitments and System Requirements 8

Components of the System 8

4. Description of Criteria, Controls, Tests and Results of Tests 19

System And Organization Controls (SOC) 2 Type 2 20

1. Independent Service Auditors' Report

To the Management of SardineAI Corp. (Sardine)

Scope

We have examined Sardine's accompanying description of its Sardine Financial Crime and Fraud Prevention, Payments, and Consortium Services titled "Description of Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services" (description) throughout the period June 1, 2025 to May 31, 2026 based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance -- 2022)* in AICPA, *Description Criteria* (description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that Sardine's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus -- 2022)* in AICPA, *Trust Services Criteria*.

Sardine uses subservice organizations to provide computing, storage, processing, and other services to support their system. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sardine, to achieve Sardine's service commitments and system requirements based on the applicable trust services criteria. The description presents Sardine's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sardine's controls. Our examination did not include the services provided by the subservice organizations, 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 Sardine, to achieve Sardine's service commitments and system requirements based on the applicable trust services criteria. The description presents Sardine's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sardine's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Sardine 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 Sardine's service commitments and system requirements were achieved.

Sardine has provided the accompanying assertion titled "Assertion of Sardine Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Sardine 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 Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the 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 operated effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

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

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

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

Inherent Limitations

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

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

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design 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 those tests are listed in section 4.

Opinion

In our opinion, in all material respects,

a. the description presents Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services that was designed and implemented throughout the period June 1, 2025 to May 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that Sardine'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 and user entities applied the complementary controls assumed in the design of Sardine's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that Sardine's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Sardine's controls operated effectively throughout that period.

Restricted Use

This report, including the description of test of controls and results thereof in section 4, is intended solely for the information and use of Sardine, user entities of Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services during some or all of the period June 1, 2025 to May 31, 2026, business partners of Sardine subject to risks arising from interactions with the Sardine Financial Crime and Fraud Prevention, Payments, and Consortium Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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



San Jose, California
October 30, 2026

Sardine

2. Assertion of Sardine Management

We have prepared the accompanying description of SardineAI Corp.'s (Sardine) Financial Crime and Fraud Prevention, Payments, and Consortium Services titled "*Description of Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services*" (description) throughout the period June 1, 2025 to May 31, 2026, based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (*With Revised Implementation Guidance -- 2022*) in AICPA, *Description Criteria* (description criteria). The description is intended to provide report users with information about the Sardine Financial Crime and Fraud Prevention, Payments, and Consortium Services that may be useful when assessing the risks arising from interactions with Sardine's system, particularly information about system controls that Sardine has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus -- 2022*) in AICPA, *Trust Services Criteria*.

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

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

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

a. the description presents Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services that was designed and implemented throughout the period June 1, 2025 to May 31, 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that Sardine'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 and user entities applied the complementary controls assumed in the design of Sardine's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period June 1, 2025 to May 31, 2026, to provide reasonable assurance that Sardine's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Sardine's controls operated effectively throughout that period.

Signed by Sardine Management

October 30, 2026

Sardine

3. Description of Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services

Company Background

SardineAI Corp. (Sardine) was founded in March 2020 with the objective of providing Financial Institutions a single platform to address their fraud and financial crime risks.

Sardine is a venture-backed company headquartered in San Francisco, California. It was founded by former early employees of Coinbase, Revolut, Uber, and PayPal with experience fighting fraud in high-risk industries.

Industries served by Sardine include financial services, cryptocurrency wallets and exchanges, payment processors, and eCommerce merchants.

Services Provided

Sardine provides Financial Crime and Fraud Prevention, Payments, and Consortium services to customers around the world. Sardine's AI platform helps prevent identity fraud at onboarding and payment fraud when funds are loaded via cards or bank accounts.

Sardine detects fraud by identifying differences between the behavior of fraudsters and that of legitimate customers. The platform can detect suspicious devices in real time, including the use of mobile emulators, remote desktop software, or proxies and VPNs. It also analyzes behavioral patterns, such as copy-and-paste activity, typing speed, and use of keyboard shortcuts, that can indicate familiarity with a platform.

Sardine's platform consists of the following:

- Device intelligence
- Behavioral biometrics
- Fraud score models running at various checkpoints
- Rules engine
- A feature store with features from phone, email, bank, and IP data providers
- Analytics and case management

Sardine also provides payment services that allow customers to implement payments infrastructure for their users, with multiple payment methods and a streamlined onboarding experience. Sardine operates as the merchant of record for these payment services.

In addition, Sardine founded Sonar, a data consortium for sharing real-time insights into first-party fraud and counterparty risk.

Sardine

Principal Service Commitments and System Requirements

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

Security commitments to user entities are documented and communicated in customer agreements and in the Terms of Service. Security commitments are standardized and include, but are not limited to, the following:

- Use of encryption technologies to protect customer data at rest and in transit.
- Operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. These requirements are communicated in Sardine's policies and procedures, system design documentation, and contracts with customers.
- Information security policies that define an organization-wide approach to how systems and data are protected. These include policies on how the service is designed and developed, how the system is operated, and how employees are hired and trained. Standard operating procedures document how to carry out specific manual and automated processes required in operation and development.

Components of the System

Infrastructure

Sardine's primary infrastructure used to provide the System includes the following:

Primary Infrastructure	
Hardware	**Purpose**
Google Cloud Platform (GCP), hosted	Hosts application servers, web servers, and data stores
Elastic Cloud, hosted	Host data for fast search and aggregation

Software

The following primary software is used to support Sardine's system.

Primary Software		
Software	**Operating Environment**	**Purpose**
Sardine API	Linux on GCP	Provides the API used by customers
Metabase	Linux on GCP	Provides dashboards

People

Sardine has a staff of over 250 full-time employees organized in the following functional areas:

- **Corporate:** executives who oversee company performance and internal reporting.
- **Product/Security:** responsible for product design and for the information security program.
- **Engineering:** responsible for building the product and monitoring its availability.
- **Sales/Strategy:** responsible for go-to-market strategy and the sales pipeline.

Data

Sardine uses Google BigQuery as its data warehouse. The main tables are:

- Customers
- Devices
- Feedback
- Transactions

Sardine uses Google Bigtable as its production database for fast querying by its web services. The main tables are:

- Biometrics
- Device Profile
- Device-Fingerprint

Processing is initiated in two ways:

- A customer makes a web request to one of our APIs, for signals and scores related to the customer or device profile
- A customer embeds Sardine's JavaScript in its web pages, which collects data in a streaming fashion and makes web requests to Sardine's web servers.

In both cases, the information provided by the customer, together with additional information Sardine obtains from data providers, is sent to an asynchronous message queue. From the message queue, the data is written to three main destinations:

- Google BigQuery, for analytics

- Google Bigtable, for fast retrieval of data for customer web requests
- Elasticsearch, where data is further transformed and aggregated to develop fraud signals.

Sardine's GCP infrastructure runs within a Virtual Private Cloud. Customer data is encrypted at rest in Sardine's datastores.

Transactions are logged using GCP Cloud Logging and GCP Error Reporting. Sardine's practices are designed to keep personally identifiable information out of logs.

Processes, Policies and Procedures

Formal policies and procedures describe logical access, computer operations, change control, and data communication standards. All personnel are expected to follow Sardine's policies and procedures, which are published on the company's internal knowledge base and available to all personnel.

Physical Security

All production data is hosted by Sardine's cloud providers. Sardine personnel have no physical access to the providers' data centers. Physical security of data center facilities is the responsibility of the subservice organization.

Logical Access

Sardine uses role-based access controls, and users must be identified and authenticated before using any system resources. Each user has a unique ID.

Sardine uses Google Workspace as its single sign-on provider for tools such as GCP, Asana, and GitHub, and requires multi-factor authentication for access to sensitive systems. Only personnel with approved access can deploy code.

New hires and other new access requests are approved during onboarding or by authorized system owners before access is granted.

When personnel leave Sardine, a formal offboarding process with a termination checklist is followed to revoke system access and recover company devices and information assets in a timely manner.

At least annually, Sardine reviews user access to its critical systems to confirm that access remains appropriate, and modifies or removes access where required.

Customer users access the Sardine Dashboard over the internet using encrypted (TLS) connections and must authenticate before gaining access.

Computer Operations – Backups

Daily backups of production data are performed and monitored to support recoverability. Sardine also replicates critical system components to support system availability and recovery objectives in the event of a failure.

Computer Operations – Availability

Sardine uses Google Cloud monitoring and alerting to identify, manage, and respond to incidents involving its infrastructure. On-call engineers are available 24/7 to respond to alerts. Vulnerabilities in Sardine's cloud infrastructure are identified through continuous scanning and remediated based on risk and impact.

Change Control

Sardine maintains documented System Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change requests, documentation requirements, development practices, quality assurance testing requirements, and required approvals.

Code changes are tested before implementation, and automated testing is performed in the continuous integration environment. Development and testing are performed in an environment that is logically separated from production. Releases are approved by appropriate personnel before they are deployed to production.

Version control software is used to manage source code and to move code through the development process to production. It maintains a history of code changes, tracks changes by developer, and supports rollback.

Data Communications

Sardine uses Google VPC firewall rules to restrict network traffic to approved communication channels and protocols, and uses Cloud NAT to manage internal IP addresses. Traffic to Sardine's load balancers is logged, and infrastructure logging is configured with automated alerts for anomalous activity. An intrusion detection system monitors the environment for potential security breaches.

An independent third party performs a penetration test of the production environment annually, and identified vulnerabilities are remediated in accordance with defined SLAs. GCP's automated vulnerability scanning is used to identify vulnerabilities in virtual machines and containers.

Boundaries of the System

The scope of this report includes the services performed by Sardine. This report does not include the data center hosting services provided by GCP.

The applicable trust services criteria and the related controls:

The Trust Services Categories that are in scope for the purposes of this report are as follows:

- **Security**: Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability or confidentiality of information or systems and affect the entity's ability to meet its objectives.
- **Availability**: Information and systems are available for operation and use to meet the entity's objectives.
- **Confidentiality**: Information designated as confidential is protected to meet the entity's objectives.

Control Environment

Integrity and Ethical Values

Integrity and ethical values are essential elements of Sardine's control environment, affecting the design, administration, and monitoring of other components. 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 communicating entity values and behavioral standards to personnel through policy statements and codes of conduct, and by example.

Specific control activities Sardine has implemented in this area include:

- A formal Code of Conduct, approved by management, communicates entity values and behavioral standards to personnel.
- Employees acknowledge the Code of Conduct, the Acceptable Use Policy, and Sardine's information security policies upon hire.
- A confidentiality statement prohibiting disclosure of proprietary or confidential information, including client information, to unauthorized parties is part of the employee handbook.
- Background checks are performed for new hires as a condition of employment, as permitted by local laws.

Commitment to Competence

Sardine's management defines competence as the knowledge and skills necessary to accomplish the tasks that define employees' roles and responsibilities. Management's commitment to competence includes considering the competence levels required for each job and how those levels translate into required skills and knowledge.

Specific control activities Sardine has implemented in this area include:

- Positions have written job descriptions listing the required qualifications, skills, and experience.
- Full-time employees complete security awareness training annually.

Sardine

Management's Philosophy and Operating Style

Sardine's management philosophy and operating style include management's approach to taking and monitoring business risks and its attitudes toward personnel.
Specific control activities Sardine has implemented in this area include:

- 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

Sardine maintains a documented organization chart that sets out roles, functional responsibilities, and reporting lines. Management has established defined roles and responsibilities to oversee implementation of the Information Security Policy across the organization.

Sardine's assignment of authority and responsibility is supported by:

- A project management system to define and track responsibilities.
- Sprint-based execution to achieve short-term goals.
- Weekly stand-up, check-in, and demo meetings.
- Slack channels for responsibility updates and clarifications.
- Notion, used to manage and distribute non-technical information within the organization.

Human Resource Policies and Practices

Sardine's human resources policies and practices cover hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities Sardine has implemented in this area include:

- New employees acknowledge the employee handbook and sign a confidentiality agreement upon hire.
- Evaluations for each employee are performed annually.
- Employee termination procedures are documented in a termination checklist.

Risk Assessment Process

Sardine's risk assessment process identifies and manages risks that could affect Sardine's ability to provide reliable services to user organizations. Sardine maintains a Risk Assessment Policy that defines risk tolerances and the process for evaluating risks against identified threats. Management performs a risk assessment annually to identify and rank potential threats to the system, including the potential for fraud and malicious acts by employees or other users. Management prepares a remediation plan to manage the resolution of findings from risk assessment activities.

Risks identified in this process include:

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

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Sardine's system; and the nature of the system's components result in risks that the criteria will not be met. Sardine addresses these risks by implementing suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and its environment are unique, the combination of risks to meeting the criteria and the controls needed to address them is also unique. As part of the design and operation of the system, Sardine's management identifies the specific risks that the criteria will not be met and the controls necessary to address them.

Information and Communications Systems

Information and communication are integral components of Sardine's internal control system. This 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. At Sardine, information is identified, captured, processed, and reported by various information systems, and through conversations with clients, vendors, regulators, and employees.

Regular meetings are held to discuss operational matters within functional areas and to communicate new policies, procedures, controls, and strategic initiatives. Updates to entity-wide security policies and procedures are communicated to the appropriate Sardine personnel. Externally, Sardine's security and availability commitments are described in its Terms of Service, and customers can report security, confidentiality, integrity, and availability failures, incidents, concerns, and other complaints through Sardine's support page.

Specific information systems used to support Sardine's system are described in the *Components of the System* section above.

Monitoring Controls

Sardine management monitors controls to confirm that they operate as intended and modifies them as conditions change. Sardine uses a continuous control monitoring platform to gain assurance that controls are in place and operating effectively, and takes corrective action based on relevant findings. Monitoring is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

On-Going Monitoring

Management's involvement in Sardine's operations helps identify significant variances from expectations regarding internal controls. Management evaluates the facts and circumstances related to any suspected control breakdown and decides whether the issue was isolated or requires a change in the company's procedures or personnel.

Reporting Deficiencies

An internal tracking tool is used to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding to and notifying management of identified risks. Corrective actions, if needed, are documented and tracked in the internal tracking tool.

Changes to the System in the Last 12 Months

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the examination period.

Criteria Not Applicable to the System

All Security, Availability, and Confidentiality Trust Services Criteria applied to Sardine's Financial Crime and Fraud Prevention, Payments, and Consortium Services.

Subservice Organizations

Sardine’s services are designed with the assumption that certain controls will be implemented by subservice organizations. These are called complementary subservice organization controls. Not all of the trust services criteria related to Sardine’s services can be achieved solely by Sardine’s control procedures. Accordingly, subservice organizations should establish their own internal controls or procedures to complement those of Sardine.

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

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity’s objectives.	

Security Category	
Criteria	Controls expected to be in place
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.	GCP is responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.4 - The entity restricts physical access to facilities and protected information assets (e.g., datacenter facilities, backup media storage and other sensitive locations) to authorized personnel to meet the entity's objectives.	GCP is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers where the entity's system resides.

Availability Category	
Criteria	*Controls expected to be in place*
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	GCP is responsible for managing environmental protections within the data centers that house network, virtualization management, and storage devices for its cloud hosting services where the entity's system resides.

Sardine management, together with the subservice organization, defines the scope and responsibility of the controls necessary to meet the relevant trust services criteria through written contracts, such as service level agreements. Sardine also monitors subservice organization controls by:

- holding periodic discussions with vendors and the subservice organization;
- reviewing attestation reports covering the services provided by vendors and the subservice organization; and
- monitoring external communications, such as customer complaints, relevant to the services provided by the subservice organization.

Complementary User Entity Controls

Sardine's services are designed with the assumption that certain controls will be implemented by user entities. These are called complementary user entity controls. Not all of the trust services criteria related to Sardine's services can be achieved solely by Sardine's control procedures. Accordingly, user entities should establish their own internal controls or procedures to complement those of Sardine.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the trust services criteria described in this report are met. These items are only part of the control considerations that may be relevant at user entities' locations, so user entities' auditors should use judgment in selecting and reviewing them.

User entities are responsible for:

- Understanding and complying with their contractual obligations to Sardine;
- Notifying Sardine of changes to technical or administrative contact information;
- Maintaining their own systems of record;
- Supervising, managing, and controlling their personnel's use of Sardine services;
- Developing their own disaster recovery and business continuity plans that address the inability to access or use Sardine services;

- Providing Sardine with a list of approvers for security and system configuration changes for data transmission; and
- Immediately notifying Sardine of any actual or suspected information security breaches, including compromised user accounts and accounts used for integrations and secure file transfers.

4. Description of Criteria, Controls, Tests and Results of Tests

Relevant trust services criteria and Sardine related controls are an integral part of management's system description and are included in this section. Sensiba LLP performed testing to determine if Sardine's controls were suitably designed and operating effectively to achieve the specified criteria for Security, Availability, and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus -- 2022*) in AICPA, *Trust Services Criteria*, throughout the period June 1, 2025 to May 31, 2026.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Sardine activities and operations and inspection of Sardine documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Sensiba LLP's testing of the controls designed to achieve the relevant trust services criteria. As inquiries were performed for substantially all Sardine controls, this test was not listed individually for every control in the tables below.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.0 - Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The entity has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to employees. Inspected the policy acknowledgements for a sample of new hires to determine that employees must accept the Code of Conduct upon hire.	No exceptions noted.
CC1.1.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	Inspected the background checks for a sample of new hires to determine that background checks were completed for new hires as a condition of their employment, as permitted by local laws.	No exceptions noted.
CC1.1.3	The entity has policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to employees. Employees must accept the Acceptable Use Policy upon hire.	Inspected the entity's Acceptable Use Policy to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to employees. Inspected the policy acknowledgements for a sample of new hires to determine that employees must accept the Acceptable Use Policy upon hire.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2.1	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of the Information Security Policy across the organization.	No exceptions noted.
CC1.2.2	The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	No exceptions noted.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	No exceptions noted.
CC1.3.2	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of the Information Security Policy across the organization.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	Entity positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the entity.	Inspected a sample job description to determine the entity's positions have a detailed job description that lists qualifications, such as requisite skills and experience, which candidates must meet in order to be hired by the entity.	No exceptions noted.
CC1.4.2	New hires are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	Inspected the background checks for a sample of new hires to determine that background checks were completed for new hires as a condition of their employment, as permitted by local laws.	No exceptions noted.
CC1.4.3	The entity has established training programs around information security to help employees understand their obligations and responsibilities to comply with the entity's security policies and procedures. Full-time employees are required to complete the training on an annual basis.	Inspected the security awareness training confirmation for a sample of full-time employees to determine that security awareness training was provided on an annual basis.	No exceptions noted.
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The entity has established training programs around information security to help employees understand their obligations and responsibilities to comply with the entity's security policies and procedures. Full-time employees are required to complete the training on an annual basis.	Inspected the security awareness training confirmation for a sample of full-time employees to determine that security awareness training was provided on an annual basis.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.5.2	The entity has approved security policies, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that employees agree to these procedures when hired.	No exceptions noted.
CC1.5.3	The entity has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to employees. Inspected the policy acknowledgements for a sample of new hires to determine that employees must accept the Code of Conduct upon hire.	No exceptions noted.
CC1.5.4	Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	Inspected the Information Security Policy to determine that management has established defined roles and responsibilities to oversee implementation of the Information Security Policy across the organization.	No exceptions noted.
CC2.0 - Communication and Information			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The entity performs continuous control monitoring to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the continuous control monitoring dashboard to determine that the entity performs control monitoring to gain assurance that controls are in place and operating effectively.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The entity has a formal Code of Conduct approved by management and accessible to employees. Employees must accept the Code of Conduct upon hire.	Inspected the entity's Code of Conduct to determine that the entity had a formal Code of Conduct approved by management and accessible to employees. Inspected the policy acknowledgements for a sample of new hires to determine that employees must accept the Code of Conduct upon hire.	No exceptions noted.
CC2.2.2	The entity has approved security policies, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that employees agree to these procedures when hired.	No exceptions noted.
CC2.2.3	The entity has policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to employees. Employees must accept the Acceptable Use Policy upon hire.	Inspected the entity's Acceptable Use Policy to determine that the entity had policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to employees. Inspected the policy acknowledgements for a sample of new hires to determine that employees must accept the Acceptable Use Policy upon hire.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC2.2.4	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The entity maintains a Terms of Service that is available to external users and internal employees, and the terms detail the entity's security and availability commitments regarding the systems.	Inspected the entity's Terms of Service to determine that it is available to external users and internal employees, and the terms detail the entity's security and availability commitments regarding the systems.	No exceptions noted.
CC2.3.2	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC2.3.3	The entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Inspected the support page to determine that the entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC3.0 - Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.1.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC3.1.3	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.2.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC3.2.3	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC3.2.4	The entity maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the annual vendor review to determine that the entity maintains a directory of its key vendors, including their annual review of vendor compliance reports.	No exceptions noted.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC3.3.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC3.3.3	The risk assessment process considers the potential for fraud, including malicious acts of employees or other users of the system.	Inspected the risk assessment to determine that the risk assessment process considered the potential for fraud, including malicious acts of employees or other users of the system.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between the board of directors and management.	No exceptions noted.
CC3.4.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC3.4.3	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC4.0 - Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	Vulnerability scans are performed on a real-time basis to identify vulnerabilities and identified vulnerabilities are remediated based on risk and impact.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed real-time to identify security issues and were remediated based on risk and impact.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC4.1.2	The entity's penetration testing is performed annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the annual penetration test performed on the in-scope environment to determine that the entity engages with a third-party to conduct penetration tests of the production environment annually and remediates vulnerabilities in accordance with SLAs.	No exceptions noted.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2.1	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC4.2.2	The entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	Inspected the support page to determine that the entity provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	No exceptions noted.
CC4.2.3	Vulnerability scans are performed on a real-time basis to identify vulnerabilities and identified vulnerabilities are remediated based on risk and impact.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed real-time to identify security issues and were remediated based on risk and impact.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC4.2.4	The entity's penetration testing is performed annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the annual penetration test performed on the in-scope environment to determine that the entity engages with a third-party to conduct penetration tests of the production environment annually and remediates vulnerabilities in accordance with SLAs.	No exceptions noted.
CC5.0 - Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC5.1.2	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC5.1.3	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	Vulnerability scans are performed on a real-time basis to identify vulnerabilities and identified vulnerabilities are remediated based on risk and impact.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed real-time to identify security issues and were remediated based on risk and impact.	No exceptions noted.
CC5.2.2	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC5.3.2	The entity has approved security policies, and employees accept these procedures when hired. Management also ensures that security policies are accessible to employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that employees agree to these procedures when hired.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.0 - Logical and Physical Access Controls			
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1.1	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected user accounts to determine that access to corporate network, production machines, network devices, and support tools requires a unique ID.	No exceptions noted.
CC6.1.2	Multi-factor authentication is required for access to sensitive systems.	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	No exceptions noted.
CC6.1.3	Role-based security is in place for internal and external users, including super admin users.	Inspected user groups and roles to determine that role-based security is in place for internal and external users, including super admin users.	No exceptions noted.
CC6.1.4	The entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	Inspected the hard-disk encryption configurations for a sample of workstations to determine that the entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	No exceptions noted.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC6.2.1	New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted.	Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.2.2	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked within a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked within a timely manner.	No exceptions noted.
CC6.2.3	Role-based security is in place for internal and external users, including super admin users.	Inspected user groups and roles to determine that role-based security is in place for internal and external users, including super admin users.	No exceptions noted.
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted.	Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted.	No exceptions noted.
CC6.3.2	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked within a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked within a timely manner.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.3.3	Annual reviews of the entity's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.	Inspected the annual user access review to determine that annual reviews of the entity's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required.	No exceptions noted.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4.1	The production environment is hosted in the cloud, thereby no onsite physical access is permitted and physical access controls are carved out of this report and are the responsibility of the subservice organization.	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			
CC6.5.1	The entity has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the disposal policies and procedures to determine that formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted.
CC6.5.2	A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked within a timely manner.	Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked within a timely manner.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The entity implements network access restrictions that ensure only approved communication channels and protocols can be used.	Inspected the network access restrictions to determine that the entity implemented network access restrictions that ensured only approved communication channels and protocols could be used.	No exceptions noted.
CC6.6.2	Multi-factor authentication is required for access to sensitive systems.	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	No exceptions noted.
CC6.6.3	The entity uses an intrusion detection system to provide continuous monitoring of the entity's network and early detection of potential security breaches.	Inspected the implemented intrusion detection system (IDS) and configurations to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6.4	The entity uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inspected the TLS configurations to determine that the entity uses appropriate encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	No exceptions noted.
CC6.6.5	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
CC6.7.1	The entity uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	Inspected the TLS configurations to determine that the entity uses appropriate encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	No exceptions noted.
CC6.7.2	Customer data at rest is encrypted.	Inspected the encryption configurations for data at rest to determine that customer data at rest is encrypted.	No exceptions noted.
CC6.7.3	The entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	Inspected the hard-disk encryption configurations for a sample of workstations to determine that the entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	No exceptions noted.
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	Antivirus software is installed on workstations to protect against malware.	Inspected the antivirus software configurations for a sample of workstations to determine that antivirus software was installed on workstations to protect against malware.	No exceptions noted.
CC6.8.2	The entity implements network access restrictions that ensure only approved communication channels and protocols can be used.	Inspected the network access restrictions to determine that the entity implemented network access restrictions that ensured only approved communication channels and protocols could be used.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.8.3	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted.
CC6.8.4	The entity has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted.
CC7.0 - System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
CC7.1.1	Vulnerability scans are performed on a real-time basis to identify vulnerabilities and identified vulnerabilities are remediated based on risk and impact.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed real-time to identify security issues and were remediated based on risk and impact.	No exceptions noted.
CC7.1.2	The entity's penetration testing is performed annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the annual penetration test performed on the in-scope environment to determine that the entity engages with a third-party to conduct penetration tests of the production environment annually and remediates vulnerabilities in accordance with SLAs.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC7.1.3	The entity has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2.1	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.	No exceptions noted.
CC7.2.2	Vulnerability scans are performed on a real-time basis to identify vulnerabilities and identified vulnerabilities are remediated based on risk and impact.	Inspected the scan results and on-going remediation to determine that vulnerability scans were performed real-time to identify security issues and were remediated based on risk and impact.	No exceptions noted.
CC7.2.3	The entity has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3.1	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.
CC7.3.2	The entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident tickets for a sample of security & privacy incidents to determine that the entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Non-Occurrence: A security or privacy incident did not occur during June 1, 2025, to May 31, 2026, so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the Incident Response Policy and security incident tracking tool to confirm the control was appropriately designed.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
CC7.4.1	The entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident tickets for a sample of security & privacy incidents to determine that the entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Non-Occurrence: A security or privacy incident did not occur during June 1, 2025, to May 31, 2026, so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the Incident Response Policy and security incident tracking tool to confirm the control was appropriately designed.
CC7.4.2	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC7.4.3	The incident response plans are tested annually to confirm they provide an effective response to potential incidents.	Inspected the annual response plan test to determine that the incident response plans were tested annually to confirm they provided an effective response to potential incidents.	No exceptions noted.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The entity has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.
CC7.5.2	The entity has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the entity has defined proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted.
CC7.5.3	Daily backups are performed and monitored to support the recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support the recoverability of the production data.	No exceptions noted.
CC7.5.4	The entity has an established Incident Response Plan that outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	Inspected the entity's Incident Response Plan to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC7.5.5	The entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Inspected the incident tickets for a sample of security & privacy incidents to determine that the entity follows a formal incident management process that includes logging, classifying, and tracking security & privacy incidents through to resolution with lessons learned devised to prevent recurrence.	Non-Occurrence: A security or privacy incident did not occur during June 1, 2025, to May 31, 2026, so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the Incident Response Policy and security incident tracking tool to confirm the control was appropriately designed.
CC7.5.6	The incident response plans are tested annually to confirm they provide an effective response to potential incidents.	Inspected the annual response plan test to determine that the incident response plans were tested annually to confirm they provided an effective response to potential incidents.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC8.0 - Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The entity has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	Inspected the Software Development Life Cycle Policy to determine that the entity has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	No exceptions noted.
CC8.1.2	Version control software is used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	Inspected the version control software to determine that version control software was used to manage source code, track changes to source code, and roll back changes following an unsuccessful implementation.	No exceptions noted.
CC8.1.3	The entity ensures that code changes are tested prior to implementation to ensure quality and security.	Inspected the test results for a sample of change tickets to determine that code changes were tested prior to implementation.	No exceptions noted.
CC8.1.4	The entity's releases are approved by appropriate personnel prior to the release being implemented in production.	Inspected the change tickets for a sample of changes to determine that releases were approved by appropriate personnel prior to the release being implemented in production.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC9.0 - Risk Mitigation			
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The entity has defined a formal risk management process that specifies risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	Inspected the Risk Assessment Policy to determine that the entity had a defined, formal risk management process that specified risk tolerances and the process for evaluating risks based on identified threats and the specified tolerances.	No exceptions noted.
CC9.1.2	A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	Inspected the risk assessment to determine that a risk assessment was completed on an annual basis and identified and ranked potential threats to the system.	No exceptions noted.
CC9.1.3	The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	Inspected the remediation plan to determine that management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	No exceptions noted.
CC9.1.4	The entity has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the entity has defined proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted.
CC9.1.5	The entity has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	Inspected the Disaster Recovery Plan to determine that business and system recovery plans were documented and included roles and responsibilities and detailed procedures for recovery of systems.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
CC9.1.6	The entity conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that the entity conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted.
CC9.1.7	The entity implements infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	Inspected the redundancy configurations to determine that the entity implemented infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	No exceptions noted.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The entity maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	Inspected the annual vendor review to determine that the entity maintains a directory of its key vendors, including their annual review of vendor compliance reports.	No exceptions noted.
CC9.2.2	The entity has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data requirements.	Inspected the Vendor Management Policy to determine that the entity has a defined Vendor Management Policy that establishes requirements of ensuring third-party entities meet the organization's data requirements.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
A1.0 - Additional Criteria for Availability			
A1.1 - The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1.1	The entity has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	Inspected the infrastructure monitoring configurations and monitoring rulesets to determine that cloud infrastructure was monitored and alerts would be sent based on predefined rulesets.	No exceptions noted.
A1.1.2	The entity implements infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	Inspected the redundancy configurations to determine that the entity implemented infrastructure redundancy by replicating critical system components to ensure system availability and support recovery objectives in the event of a failure.	No exceptions noted.
A1.2 - The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.			
A1.2.1	The entity relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's compliance reporting efforts.	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3.1	Daily backups are performed and monitored to support the recoverability of the production data.	Inspected the daily backup configuration to determine that daily backups were performed and monitored to support the recoverability of the production data.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
A1.3.2	The entity conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.	Inspected the business continuity and disaster recovery tests to determine that the entity conducted annual business continuity and disaster recovery tests to ensure the response plans were effective.	No exceptions noted.
A1.3.3	The entity has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	Inspected the Business Continuity Plan to determine that the entity has defined proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted.
C1.0 - Additional Criteria for Confidentiality			
C1.1 - The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1.1	The entity establishes written policies related to retention periods for the confidential information it maintains.	Inspected the Data Retention Policy to determine that the entity established written policies related to retention periods for the confidential information it maintains.	No exceptions noted.
C1.1.2	The entity has established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that are required.	Inspected the Data Classification Policy to determine that the entity had established a data classification policy in order to identify the types of confidential information possessed by the entity and types of protection that were required.	No exceptions noted.
C1.1.3	Customer data at rest is encrypted.	Inspected the encryption configurations for data at rest to determine that customer data at rest is encrypted.	No exceptions noted.

Criteria Number	Description of Company Controls	Service Auditor's Test of Controls	Result
C1.1.4	Access to corporate network, production machines, network devices, and support tools requires a unique ID.	Inspected user accounts to determine that access to corporate network, production machines, network devices, and support tools requires a unique ID.	No exceptions noted.
C1.1.5	The entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	Inspected the hard-disk encryption configurations for a sample of workstations to determine that the entity's workstations have hard-disk encryption applied to protect locally stored data and access credentials.	No exceptions noted.
C1.2 - The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2.1	The entity has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	Inspected the disposal policies and procedures to determine that formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	No exceptions noted.