LOGIXBOARD

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

Software as a Service System

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to Trust Services Criteria for Security

For the period 1 March 2025 to 28 February 2026

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Logixboard, Inc (Logixboard)

Scope

We have examined Logixboard's accompanying description of its Software as a Service System titled "Description of Logixboard's Software as a Service System" (description) throughout the period 1 March 2025 to 28 February 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 1 March 2025 to 28 February 2026, to provide reasonable assurance that Logixboard's service commitments and system requirements were achieved based on:

- the Trust Services Criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (*With Revised Points of Focus — 2022)* in AICPA, *Trust Services Criteria*.

Logixboard 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 Logixboard, to achieve Logixboard's service commitments and system requirements based on the applicable trust services criteria. The description presents Logixboard's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Logixboard'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 Logixboard, to achieve Logixboard's service commitments and system requirements based on the applicable trust services criteria. The description presents Logixboard's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Logixboard'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

Logixboard 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 Logixboard's service commitments and system requirements were achieved. Logixboard has provided the accompanying assertion titled "Assertion of Logixboard Management" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Logixboard 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 the 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 Logixboard's Software as a Service System that was designed and implemented throughout the period 1 March 2025 to 28 February 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period 1 March 2025 to 28 February 2026, to provide reasonable assurance that Logixboard'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 Logixboard's controls throughout that period.
c. the controls stated in the description operated effectively throughout the period 1 March 2025 to 28 February 2026 to provide reasonable assurance that Logixboard's service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Logixboard'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 Logixboard, user entities of Logixboard's Software as a Service System during some or all of the period 1 March 2025 to 28 February 2026, business partners of Logixboard subject to risks arising from interactions with the Software as a Service System, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

Sensiba LLP

San Jose, California
13 April 2026

2. Assertion of Logixboard Management

We have prepared the accompanying description of Logixboard, Inc's (Logixboard) Software as a Service System titled "Description of Logixboard's Software as a Service System" (description) throughout the period 1 March 2025 to 28 February 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 Software as a Service System that may be useful when assessing the risks arising from interactions with Logixboard's system, particularly information about system controls that Logixboard 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 (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*.

Logixboard 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 Logixboard, to achieve Logixboard's service commitments and system requirements based on the applicable trust services criteria. The description presents Logixboard's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Logixboard'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 Logixboard, to achieve Logixboard's service commitments and system requirements based on the applicable trust services criteria. The description presents Logixboard's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Logixboard's controls.

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

a. the description presents Logixboard's Software as a Service System that was designed and implemented throughout the period 1 March 2025 to 28 February 2026, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period 1 March 2025 to 28 February 2026, to provide reasonable assurance that Logixboard'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 Logixboard's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period 1 March 2025 to 28 February 2026 to provide reasonable assurance that Logixboard's service commitments and system requirements were achieved based on the applicable trust services criteria, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Logixboard's controls operated effectively throughout that period.

Signed by Logixboard Management

13 April 2026

3. Description of Logixboard's Software as a Service System

Company Background

Logixboard, Inc. ("Logixboard") is a software company founded in 2016 that provides a cloud-based platform designed to improve visibility, communication, and operational efficiency for logistics service providers and their customers. Logixboard enables freight forwarders and logistics companies to deliver modern digital experiences to their customers through real-time tracking, collaboration, and workflow automation tools.

Logixboard primarily serves logistics providers and their customers globally, supporting operations across supply chain visibility, shipment tracking, and customer engagement.

Services Provided

Logixboard provides a Software as a Service (SaaS) platform that enables logistics companies to manage and share shipment data with their customers through a centralized, secure interface.

The Logixboard platform includes core web-based applications as well as supporting tools such as Clockwork, an Outlook add-in designed to improve communication workflows by integrating shipment visibility and operational data directly into email interactions.

Core platform capabilities include:

- Real-time shipment tracking and visibility
- Customer-facing dashboards and portals
- Automated notifications and alerts
- Document management and sharing
- Workflow and collaboration tools

Logixboard's platform integrates with customer systems and third-party data sources to aggregate and present shipment and operational data in a unified experience.

The platform is delivered via a web-based interface and supported by cloud infrastructure, enabling scalability, availability, and secure access for authorized users.

Principal Service Commitments and System Requirements

Logixboard has established processes, policies, and procedures to meet its objectives related to its Software as a Service System (the 'System'). Those objectives are based on the purpose, vision, and values of Logixboard as well as commitments that Logixboard makes to user entities, the requirements of laws and regulations that apply to Logixboard's activities, and the operational requirements that Logixboard has established.

Commitments are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Logixboard's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

Components of the System

Infrastructure
Logixboard's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of AWS.

System	Type	Description
Amazon Elastic Compute Cloud (EC2)	Cloud Compute	Secure and resizable compute capacity (virtual servers) in the cloud.
Amazon Elastic Container Service (ECS)	Cloud Compute	Secure, reliable, and scalable service to run containers.
Amazon Elastic Kubernetes Service (EKS)	Cloud Compute	Fully managed Kubernetes service.
AWS Lambda	Cloud Compute	Serverless, event-driven compute service.
AWS Fargate	Cloud Compute	Serverless compute for containers.
PostgreSQL	Data Storage	Open-source relational database management system emphasizing extensibility and SQL compliance.
Amazon RDS	Data Storage	Relational database service.
Amazon DynamoDB	Data Storage	Key value database service.
Amazon Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
AWS Web Application Firewall	Web Application Firewall	Protects web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources.
AWS Elastic Load Balancing (ELB)	Networking	Automatically distributes incoming application traffic across multiple targets.

System	Type	Description
Amazon API Gateway	Networking	Service to create, maintain, and secure application programming interfaces (API's).
AWS CloudFront	Content Delivery Network	Low-latency, global delivery of content.
AWS Certificate Manager	Encryption	A service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services.
AWS Key Management Service	Key Management	Centralized control over the cryptographic keys used to protect data.

Software

Primary software is used to support Logixboard's system.

Software	Purpose
Logixboard, Clockwork	The Software as a Service System provided to Logixboard customers.
AWS CloudTrail	Enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage on AWS.
AWS CloudWatch	Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources.
AWS GuardDuty	Threat detection service that continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation.
Amazon Inspector	Automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
Okta	Authentication software used to identify and authenticate users for access control to the systems.
GitHub, AWS	Source code repository used to manage the software code and version control.
Gitlab/Spacelift	Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment.
1Password	Enterprise password manager used to store authentication secrets and strengthen password security.

Software	Purpose
Kandji, Intune	Mobile device management software used to track and manage security policies on endpoint devices.
Kandji Avert EDR,	Anti-virus software used to protect endpoint devices from malware.
Data Dog	System monitoring software used to log events and raise alerts to support system security and availability.
JIRA, Linear	Ticketing software used to log events and requirements to support the internal controls.
Trinet (Zenefits)	Human resources information system used to manage employee processes like onboarding, offboarding and performance.
Google Workspace	Google's suite of enterprise productivity, collaboration, and communication tools.
Drata	Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance.

People

Logixboard's personnel are organized into the following functional areas:

- Leadership: The executive level responsible for corporate governance.
- Product: Responsible for managing the roadmap of requirements and balancing the Engineering team priorities.
- Engineering: Responsible for building and maintaining the infrastructure and software.
- Customer Success: Responsible for the customer experience, support, and services.
- Implementations: Responsible for enterprise implementations and integrations to onboard and set up new customers.
- Project Management: Responsible for enterprise delivery of programs and projects to support the objectives.
- Operations: Responsible for monitoring and supporting robust and effective company and system operations.
- Risk and Compliance: Responsible for identification, assessment, treatment and monitoring to manage risks and support compliance.
- Partnerships: Responsible for managing partnerships with complementary service providers.
- Sales: Responsible for onboarding new customers and aligning requirements.
- Marketing: Responsible for branding, market positioning and attracting customers.

Data

The data collected and processed by Logixboard includes the following types:

- Basic personal details: name, email, contact details.
- User activity: user activity within the software.

Processes, Policies and Procedures
Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Logixboard's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Logixboard's employees and can be referred to as needed.

Compliance Management Platform
Logixboard uses compliance automation software, Drata, to support the design, implementation, operation, monitoring, and documentation of internal controls. Drata leverages APIs to centralize the monitoring of Logixboard's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Drata support the continuous monitoring of control activities for Logixboard's people, devices, policies, procedures and plans, risk assessments, third-party vendor assessments, system monitoring and the security configurations of these critical systems.

Using Drata does not reduce management's responsibility for designing, implementing, and operating an effective system of internal control. Logixboard evaluates the accuracy and completeness of the information stored in Drata and conducts annual vendor risk assessments.

Physical Security
The critical infrastructure and data of the System are hosted by AWS. There are no trusted local office networks. As such, AWS is responsible for the key physical security controls that support the System.

Logical Access
Logixboard's logical access processes restrict access to the infrastructure, software, and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfil job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. Okta authentication software is used for identity management and single sign-on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are periodically reviewed and adjusted when no longer required. Additional information security policies and procedures require Logixboard employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, periodic testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Logixboard employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Kandji, Intune mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

System Operations
Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Logixboard's critical infrastructure and data are hosted by AWS with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery in continuity considerations are built into the system design of AWS to support Logixboard's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

Change Control
Logixboard operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the Logixboard, Clockwork software to support Logixboard's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub, AWS version control software is used for the code repository that tracks all changes to the Logixboard, Clockwork software, including managing versions and roll-back capability in the event of a failed change release.

A continuous integration / continuous deployment (CI/CD) pipeline is configured using Gitlab/Spacelift to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

Data Governance
Logixboard uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of Logixboard.

Established processes, policies, procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

Control Environment

Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Logixboard's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Logixboard's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

Commitment to Competence

Logixboard's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Logixboard's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

Management's Philosophy and Operating Style

Logixboard's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Logixboard's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

Organizational Structure and Assignment of Authority and Responsibility

Logixboard's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Logixboard's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies, and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

Human Resource Policies and Practices

Logixboard's employees are the foundation for achieving the objectives and commitments. Logixboard's hiring, onboarding and human resource practices are designed to attract, develop,

and retain high-quality employees. That includes training and development, performance evaluations, compensation, and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

Risk Assessment Process

Logixboard's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Logixboard, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Logixboard's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance risk – legal and regulatory obligations and changes.
- Financial risk – the sustainability of Logixboard and resources supporting the objectives.

These risks are identified by Logixboard management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Logixboard's context.

Integration with Risk Assessment

Established internal controls include Logixboard's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as Logixboard grows, and the associated risks change.

Information and Communications Systems

Information and communication are a core part of Logixboard's internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control Logixboard's operations effectively. The information and communication systems consider the internal control requirements, operating requirements,

and the needs of interested parties including employees, customers, third-party vendors, regulators, and shareholders.
The information and communication systems include central tracking systems that support Logixboard's established processes, as well as various meetings, and documented policies, procedures, and organizational knowledge.

Monitoring Controls

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Logixboard's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the board, for ensuring appropriate actions are completed in a timely manner.

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 Trust Services Criteria were applicable to Logixboard's Software as a Service System.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS.

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

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

Subservice Organization – AWS		
Category	Criteria	Control
Security	CC6.1-CC6.8	Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches.
Security	CC6.4	Policies and procedures are established and followed to restrict physical access to data center facilities, backup media, and other system components, including firewalls, routers, and servers.
Security	CC7.1-CC7.5	Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events.
Security	CC8.1	Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production.

Logixboard management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Logixboard performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

Complementary User Entity Controls

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

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

User entities are responsible for:

- Understanding and complying with Logixboard's terms of service.
- Notifying Logixboard of changes made to technical or administrative contact information.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Ensuring multi-factor authentication is applied by personnel, if required.
- Ensuring the supervision, management, and control of the use of Logixboard's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Logixboard services for any critical reliance on these services.

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

Relevant trust services criteria and Logixboard related controls are an integral part of management's system description and are included in this section. Sensiba LLP performed testing to determine if Logixboard's controls were suitably designed and operating effectively to achieve the specified criteria for Security 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 1 March 2025 to 28 February 2026.

Tests of the controls included inquiry of appropriate management, supervisory and staff personnel, observation of Logixboard activities and operations and inspection of Logixboard 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 Logixboard controls, this test was not listed individually for every control in the tables below.

Common Criteria 1: Control Environment

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The entity has a formal Code of Conduct approved by management and accessible to all employees. All 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 all employees.	No exceptions noted
			Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Code of Conduct upon hire.	No exceptions noted
		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 all new hires as a condition of their employment.	No exceptions noted
		The entity has policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to all employees. All 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 all employees.	No exceptions noted
			Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Acceptable Use Policy upon hire.	No exceptions noted

CC1.0	Criteria	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.	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
		The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between management and the senior 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 management and the senior management.	No exceptions noted
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate	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

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	authorities and responsibilities in the pursuit of objectives.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between management and the senior 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 management and the senior management.	No exceptions noted
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	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 all new hires as a condition of their employment.	No exceptions noted
		All 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.	Inspected a sample job description to determine that job requirements and responsibilities were documented.	No exceptions noted

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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. All 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 completed 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.	The entity has a formal Code of Conduct approved by management and accessible to all employees. All 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 all employees.	No exceptions noted
			Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Code of Conduct upon hire.	No exceptions noted
		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

CC1.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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. All 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 completed on an annual basis.	No exceptions noted
		The entity has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted

Common Criteria 2: Information and Communication

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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
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.	The entity has a formal Code of Conduct approved by management and accessible to all employees. All 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 all employees.	No exceptions noted
			Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Code of Conduct upon hire.	No exceptions noted
		The entity has policies and procedures in place to establish acceptable use of information assets approved by management and is accessible to all employees. All employees	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 all employees.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		must accept the Acceptable Use Policy upon hire.	Inspected the policy acknowledgements for a sample of new hires to determine that all employees must accept the Acceptable Use Policy upon hire.	No exceptions noted
		The entity has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
		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	The entity maintains a Terms of Service that is available to all 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 all external users and internal employees, and the terms detail the entity's security and availability commitments regarding the systems.	No exceptions noted

CC2.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	functioning of internal control.	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
		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

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	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
		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
		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	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

CC3.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	risks as a basis for determining how the risks should be managed.	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
		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
		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 security documentation, including compliance reports, are collected from sub-service organizations and key vendors.	No exceptions noted
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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
		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

CC3.0	Criteria	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.	The documented organization chart outlines the roles, functional responsibilities and reporting lines for the entity personnel and demonstrates independence between management and the senior 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 management and the senior management.	No exceptions noted
		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
		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

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Vulnerability scans are performed on a continuous 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 continuous to identify security issues and were remediated based on risk and impact.	No exceptions noted
		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.	Vulnerability scans are performed on a continuous 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 continuous to identify security issues and were remediated based on risk and impact.	No exceptions noted
		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

CC4.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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
		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

Common Criteria 5: Control Activities

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	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
		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
		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
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over	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

CC5.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	technology to support the achievement of objectives.	Vulnerability scans are performed on a continuous 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 continuous to identify security issues and were remediated based on risk and impact.	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.	The entity has approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees.	Inspected the security policies and acknowledgement for a sample of new hires to determine that all employees agree to these procedures when hired.	No exceptions noted
		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

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	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
		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
		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
		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 implemented for accessing systems and resources.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	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
		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
		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 implemented for accessing systems and resources.	No exceptions noted
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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
		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
		Quarterly 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 user access review for a sample of quarters to determine that quarterly 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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	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.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by 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.	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
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC6.0	Criteria	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.	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
		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
		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
		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
		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

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
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.	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
		Customer data at rest is encrypted.	Inspected the encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of	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

CC6.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	unauthorized or malicious software to meet the entity's objectives.	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
		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
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 7: System Operations

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Vulnerability scans are performed on a continuous 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 continuous to identify security issues and were remediated based on risk and impact.	No exceptions noted
		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
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	Vulnerability scans are performed on a continuous 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 continuous to identify security issues and were remediated based on risk and impact.	No exceptions noted
		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
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

CC7.0	Criteria	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.	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
		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.	N/A – non-occurrence: There were no operating instances of this control during the examination period so auditor could not include on the operating effectiveness of the control. Auditor reviewed the Incident Management Plan to confirm the control was appropriately designed.	Testing of the control activity disclosed that there no incidents during the examination period.
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and	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

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
	communicate security incidents, as appropriate.	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.	N/A – non-occurrence: There were no operating instances of this control during the examination period so auditor could not include on the operating effectiveness of the control. Auditor reviewed the Incident Management Plan to confirm the control was appropriately designed.	Testing of the control activity disclosed that there no incidents during the examination period.
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	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

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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.	N/A – non-occurrence: There were no operating instances of this control during the examination period so auditor could not include on the operating effectiveness of the control. Auditor reviewed the Incident Management Plan to confirm the control was appropriately designed.	Testing of the control activity disclosed that there no incidents during the examination period.
		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
		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
		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

CC7.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 8: Change Management

CC8.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
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.	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 a Software Development Life Cycle Policy was defined to ensure that appropriate controls were in place over the acquisition, development, and maintenance of technology and its infrastructure.	No exceptions noted
		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
		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
		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
		Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.		

Common Criteria 9: Risk Mitigation

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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
		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
		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
		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

CC9.0	Criteria	Description of Company Controls	Service Auditor's Test of Controls	Result
		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
		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
		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.	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 security documentation, including compliance reports, are collected from sub-service organizations and key vendors.	No exceptions noted

CC9.0	Criteria	Description of Company Controls	Service Auditor’s Test of Controls	Result
		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 a vendor risk management program with a framework for managing the lifecycle of vendor relationships is defined.	No exceptions noted