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

Coderbyte Platform

And the Suitability of Design of Controls Relevant to the Controls Placed in Operation and Test of Operating Effectiveness Relevant to Security and Availability

For the period May 16, 2024 to May 15, 2025

TOGETHER WITH INDEPENDENT AUDITORS' REPORT

Prepared by:

Sensiba

Table of Contents

1. Independent Service Auditors' Report

To the Management of Coderbyte Enterprise Inc (Coderbyte)

Scope

We have examined Coderbyte's accompanying description of its Platform titled "Description of the Coderbyte Platform" (description) throughout the period May 16, 2024 to May 15, 2025 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 May 16, 2024 to May 15, 2025, to provide reasonable assurance that Coderbyte's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (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*.

The information included in Section 5 of this report is presented by management of Coderbyte to provide additional information to user entities and is not a part of the description of the system. Information included here in Section 5 has not been subjected to the procedures applied in the examination of the description of the system related to description of the system, and accordingly, Sensiba LLP expresses no opinion on it.

Coderbyte uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the applicable trust services criteria. The description presents Coderbyte's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Coderbyte'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 Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the applicable trust services criteria. The description presents Coderbyte's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Coderbyte'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

Coderbyte 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 Coderbyte's service commitments and system requirements were achieved. Coderbyte has provided the accompanying assertion titled "Assertion of Coderbyte Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Coderbyte 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 the Coderbyte Platform that was designed and implemented throughout the period May 16, 2024 to May 15, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period May 16, 2024 to May 15, 2025, to provide reasonable assurance that Coderbyte'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 Coderbyte's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period May 16, 2024 to May 15, 2025, to provide reasonable assurance that Coderbyte'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 Coderbyte'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 Coderbyte, user entities of Coderbyte's Platform during some or all of the period May 16, 2024 to May 15, 2025, business partners of Coderbyte subject to risks arising from interactions with the Platform, 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

June 18, 2025

2. Assertion of Coderbyte Management

We have prepared the accompanying description of Coderbyte Enterprise Inc's (Coderbyte) Platform titled "*Description of the Coderbyte Platform*" (description) throughout the period May 16, 2024 to May 15, 2025, 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 Platform that may be useful when assessing the risks arising from interactions with Coderbyte's system, particularly information about system controls that Coderbyte 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 and Availability (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*.

Coderbyte uses a subservice organization to provide application maintenance and support services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the applicable trust services criteria. The description presents Coderbyte's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Coderbyte'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 Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the applicable trust services criteria. The description presents Coderbyte's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Coderbyte's controls.

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

a. the description presents the Coderbyte Platform that was designed and implemented throughout the period May 16, 2024 to May 15, 2025, in accordance with the description criteria.
b. the controls stated in the description were suitably designed throughout the period May 16, 2024 to May 15, 2025, to provide reasonable assurance that Coderbyte'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 Coderbyte's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period May 16, 2024 to May 15, 2025, to provide reasonable assurance that Coderbyte'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 Coderbyte's controls operated effectively throughout that period.

Signed by Coderbyte Management

June 18, 2025

3. Description of the Coderbyte Platform

Company Background

Coderbyte Enterprise Inc. (‘Coderbyte’) was founded in June 2012 with the objective of helping companies make informed hiring decisions through aptitude testing to determine technical proficiencies. Coderbyte has created a technical assessment and interviewing Software as a Service (SaaS) platform that services 3000+ customers.

Coderbyte's focus is to serve any company that is in the process of hiring technical roles in software development and engineering, across all industries.

Services Provided

Coderbyte supports customers globally. Coderbyte’s product covers the hiring process needs for companies, for both remote and in-person capacities. Services include auto-graded technical assessments, interviewing materials, assessable projects for candidates, reporting analytics and cheating detection for tests.

Principal Service Commitments and System Requirements

Coderbyte 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 Coderbyte as well as commitments that Coderbyte makes to user entities, the requirements of laws and regulations that apply to Coderbyte’s activities, and the operational requirements that Coderbyte 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 Coderbyte’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

Coderbyte's primary infrastructure used to provide the System includes the cloud hosted networking, compute, and database components of Amazon Web Services (AWS) and Heroku.

Primary Infrastructure		
System	**Type**	**Description**
Heroku	Platform as a Service	Enables developers to build, run, and operate applications entirely in the cloud.
Amazon RDS	Data Storage	Relational database service.
AWS Simple Storage Service (S3)	Data Storage	Object, file, and block storage.
AWS Elastic Load Balancing (ELB)	Networking	Automatically distributes incoming application traffic across multiple targets.
Cloudflare	Network Services	DNS, load balancing, DDOS protection, web firewall and TLS encryption.
AWS Key Management Service	Key Management	Centralized control over the cryptographic keys used to protect data.

Software

Primary software is used to support Coderbyte's system.

Primary Software	
Software	**Purpose**
Coderbyte	The Software as a Service System provided to Coderbyte customers.
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.
AWS Inspector	Automated vulnerability management service that continually scans AWS workloads for software vulnerabilities and unintended network exposure.
GitHub	Source code repository used to manage the software code and version control.
GitHub Actions	Continuous development/continuous integration 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.

Primary Software	
Software	**Purpose**
Norton	Anti-virus software used to protect endpoint devices from malware.
New Relic	System monitoring software used to log events and raise alerts to support system security and availability.
GitHub Issues	Ticketing software used to log events and requirements to support the internal controls.
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

Coderbyte has 3 people who are organized into the following functional areas:

- Leadership: The executive level is responsible for corporate governance.
- Engineering: Responsible for building and maintaining the infrastructure and software.
- 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.

Data

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

- Basic personal details: name, email, and 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 Coderbyte's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Coderbyte's employees and can be referred to as needed.

Compliance Management Platform

Coderbyte 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 Coderbyte's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Drata supports the continuous monitoring of control activities for Coderbyte'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. Coderbyte evaluates the accuracy and completeness of the information stored in Drata and conducts annual vendor risk assessments including review of Drata's SOC 2 Type 2 reports that includes the trust services criteria related to processing integrity.

Physical Security

The critical infrastructure and data of the System is hosted by Amazon Web Services (AWS) and Heroku. There are no trusted local office networks. As such, AWS and Heroku are responsible for the key physical security controls that support the System.

Logical Access

Coderbyte'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. Google Workspace is used for single-sign-on and identity management. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are reviewed quarterly and adjusted when no longer required. Additional information security policies and procedures require Coderbyte 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, quarterly testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Coderbyte 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.

Computer Operations – Backups

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.

Computer Operations – Availability

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

Change Control

Coderbyte 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 Coderbyte software to support Coderbyte's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the Coderbyte 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 GitHub Actions 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 Communications

Coderbyte 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 Coderbyte.

Established processes, policies, and 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.

Boundaries of the System

The scope of this report includes the Coderbyte Software as a Service System (the 'System'). This report does not include the cloud hosting services provided by Amazon Web Services (AWS) and Heroku.

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.

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 Coderbyte's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Coderbyte'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

Coderbyte's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Coderbyte'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.

Management's Philosophy and Operating Style

Coderbyte's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Coderbyte'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

Coderbyte'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 Coderbyte'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

Coderbyte's employees are the foundation for achieving the objectives and commitments. Coderbyte'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

Coderbyte's risk assessment process identifies and manages risks that threaten the 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 they are aligned with the risk appetite and objectives of Coderbyte, 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 the security, reliability, and integrity of Coderbyte's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory obligations and changes.
- Financial – the sustainability of Coderbyte and resources supporting the objectives.

These risks are identified by Coderbyte 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 Coderbyte's context.

Integration with Risk Assessment

Established internal controls include Coderbyte'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 Coderbyte grows, and the associated risks change.

Information and Communications Systems

Information and communication are a core part of Coderbyte'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 Coderbyte'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 Coderbyte'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 Coderbyte'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 on remediation actions or reinforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and the Board, to ensure 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 review date.

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 review date.

Criteria Not Applicable to the System

All relevant trust services criteria were applicable to Coderbyte Platform.

Subservice Organizations

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

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

Security Category	
Criteria	Controls expected to be in place
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	AWS & Heroku are responsible for implementing controls for the transmission, movement, and removal of the underlying storage devices for its cloud hosting services where the entity's system resides.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	

Security Category	
Criteria	Controls expected to be in place
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.	AWS & Heroku are 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.	AWS & Heroku are 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.

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

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

Complementary User Entity Controls

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

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

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

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

Relevant trust services criteria and Coderbyte related controls are an integral part of management's system description and are included in this section. Sensiba LLP performed testing to determine if Coderbyte's controls were suitably designed and operating effectively to achieve the specified criteria for Security and Availability 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 May 16, 2024 to May 15, 2025.

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

Description of Company Controls	Criteria Number	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.			
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.	CC1.1.1	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. 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

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.1.2	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, posted on the company wiki, and accessible to all employees. All employees must accept the Acceptable Use Policy upon hire.	CC1.1.3	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, posted on the company wiki, and accessible to all employees. 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
CC1.2 - 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.	CC1.2.1	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

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC1.3.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.	CC1.3.2	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
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
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.	CC1.4.1	Inspected a job description to determine that job requirements and responsibilities were documented.	No exceptions noted
New employees and contractors are subjected to background and/or reference checks as a condition of their employment, as permitted by local laws.	CC1.4.2	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

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
The entity has established training programs for privacy and information security to help employees understand their obligations and responsibilities to comply with the entity's security policies and procedures, including the identification and reporting of incidents. All full-time employees are required to complete the training upon hire and annually thereafter.	CC1.5.1	Inspected security awareness training confirmation for a sample of new hires and existing employees to determine that security awareness training was provided upon hire and annually thereafter.	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 and contractors.	CC1.5.2	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

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The entity conducts continuous monitoring of security controls using Drata, and addresses issues in a timely manner.	CC2.1.1	Inspected the Drata tool configurations to determine that the company uses a SOC 2 compliance platform called Drata which objectively and continuously monitors the company's control environment and alerts management when internal control and security issues arise.	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.	CC2.2.1	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. 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 approved security policies, and all employees accept these procedures when hired. Management also ensures that security policies are accessible to all employees and contractors.	CC2.2.2	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

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
The entity maintains a Privacy Policy that is available to all external users and internal employees, and it details the company's confidentiality and privacy commitments.	CC2.3.1	Inspected the entity's website to determine that the entity's privacy policies were posted.	No exceptions noted
The company maintains a Terms of Service that is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	CC2.3.2	Inspected the company's Terms of Service to determine that it is available to all external users and internal employees, and the terms detail the company's security and availability commitments regarding the systems.	No exceptions noted
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.			
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.	CC3.1.1	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 - 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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.2.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC3.2.2	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
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.3.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
The company reviews its organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	CC3.4.1	Inspected the organization chart review to determine that management reviewed the organizational structure, reporting lines, authorities, and responsibilities in terms of information security on an annual basis.	No exceptions noted
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC3.4.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC4.1.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted
The company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC4.1.2	Inspected the penetration test results to determine that the company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	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.			
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.	CC4.2.1	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
The company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	CC4.2.2	Inspected the support page to determine that the company provides a process to external users for reporting security, confidentiality, integrity and availability failures, incidents, concerns, and other complaints.	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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC5.1.1	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	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.	CC5.1.2	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
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC5.2.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
The entity's Management prepares a remediation plan to formally manage the resolution of findings identified in risk assessment activities.	CC5.2.2	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.			
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.	CC5.3.1	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
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 and contractors.	CC5.3.2	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
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.			
Access to corporate network, production machines, network devices, and support tools requires a unique ID.	CC6.1.1	Inspected user accounts to determine that access to corporate network, production machines, network devices, and support tools requires a unique ID.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
The company requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	CC6.1.2	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	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.			
Prior to granting new hires access to system resources, HR must submit a completed access request form.	CC6.2.1	Inspected the access request form for a sample of new hires to determine that HR must submit a completed access request form prior to granting new hires access to system resources.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
A termination checklist is completed to ensure that system access, including physical access, for terminated employees has been removed within one business day.	CC6.2.2	Inspected the termination checklist for a sample of terminated employees to determine that employee access to infrastructure is removed within one business day.	N/A - Non-Occurrence: A terminated employee did not occur during May 16, 2024 to May 15, 2025 so auditor could not conclude on the operating effectiveness of the control. Auditor reviewed the System Access Control Policy and the personnel tool to confirm the control was appropriately designed.
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.			
The company's access reviews are performed on a quarterly basis.	CC6.3.1	Inspected the access review to determine that an access review was completed for the company on a quarterly basis.	No exceptions noted

Description of Company Controls	Criteria Number	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, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	CC6.4.1	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.			
The company has formal policies and procedures in place to guide personnel in the disposal of hardware containing sensitive data.	CC6.5.1	Inspected the Data Deletion Policy to determine that procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	No exceptions noted
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
The company uses firewalls that ensure only approved connections, ports, and protocols are implemented.	CC6.6.1	Inspected firewall rules to determine that inbound and outbound traffic is appropriately restricted and allowed by exception.	No exceptions noted
The company requires two factor authentication to access sensitive systems and applications in the form of user ID, password, OTP and/or certificate.	CC6.6.2	Inspected system configurations to determine that MFA was required in order to access sensitive systems and applications.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
The company uses encryption to protect user authentication and admin sessions of the internal admin tool transmitted over the Internet.	CC6.7.1	Inspected TLS configurations to determine that the company 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.	CC6.7.2	Inspected encryption configurations for data at rest to determine that customer data at rest was encrypted.	No exceptions noted
The company ensures that company-issued laptops have encrypted hard-disks.	CC6.7.3	Inspected workstation and laptop encryption settings for a sample of computers to determine that full-disk encryption was implemented for all workstations and laptops.	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.			
The company requires antivirus software to be installed on workstations to protect the network against malware.	CC6.8.1	Inspected antivirus configurations for a sample of computers to determine that antivirus software was installed on workstations to protect the network against malware.	No exceptions noted
The company uses firewalls that ensure only approved connections, ports, and protocols are implemented.	CC6.8.2	Inspected firewall rules to determine that inbound and outbound traffic is appropriately restricted and allowed by exception.	No exceptions noted

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
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.			
Vulnerability scans are performed on a quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC7.1.1	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted
The company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	CC7.1.2	Inspected the penetration test results to determine that the company engages with third-party to conduct penetration tests of the production environment at least annually. Results are reviewed by management and high priority findings are tracked to resolution.	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.			
The company uses logging software that sends alerts to appropriate personnel. Corrective actions are performed, as necessary, in a timely manner.	CC7.2.1	Inspected the infrastructure logging configurations and alerts to determine that logging is implemented and alerts are automatically created, sent to appropriate personnel and resolved, as necessary.	No exceptions noted

Description of Company Controls	Criteria Number	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 quarterly basis to identify vulnerabilities and management takes action based on the results of the scan.	CC7.2.2	Inspected the scan results to determine that vulnerability scans were performed quarterly to identify security issues quarterly and were remediated timely.	No exceptions noted
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 incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.3.1	Inspected the incident response policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted

Description of Company Controls	Criteria Number	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 company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	CC7.3.2	Inspected the incident tickets for a sample of security and privacy incidents to determine that the company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	N/A - Non-Occurrence: A security or privacy incident did not occur during May 16, 2024 to May 15, 2025 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.

Description of Company Controls	Criteria Number	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.	CC7.3.3	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted
CC7.4 - The entity responds to identified security incidents by executing a defined incident-response program to understand, contain, remediate, and communicate security incidents, as appropriate.			
The incident response team follows defined incident response procedures for resolving and escalating reported security issues.	CC7.4.1	Inspected the incident response policy to determine that policies and procedures related to resolving and escalating reported security issues were in place.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
The company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	CC7.4.2	Inspected the incident tickets for a sample of security and privacy incidents to determine that the company tracks and prioritizes security & privacy deficiencies through internal tools according to their severity by an independent technical resource.	N/A - Non-Occurrence: A security or privacy incident did not occur during May 16, 2024 to May 15, 2025 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.

Description of Company Controls	Criteria Number	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.			
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.	CC7.4.3	Inspected the entity's incident response policies and procedures to determine that it outlines management responsibilities and procedures to ensure a quick, effective, and orderly response to information security incidents.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
The company has an established Disaster Recovery Plan that outlines roles and responsibilities and detailed procedures for recovery of systems.	CC7.5.1	Inspected 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
The company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	CC7.5.2	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
The company ensures that incident response plan testing is performed on an annual basis.	CC7.5.3	Inspected the incident response exercise to determine that incident response plan testing is performed on an annual basis to ensure that procedures are complete and accurate.	No exceptions noted

Description of Company Controls	Criteria Number	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.			
The company has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes.	CC8.1.1	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.	CC8.1.2	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 company ensures that code changes are tested prior to implementation to ensure quality and security.	CC8.1.3	Inspected test results for a sample of changes to determine that code changes were tested prior to implementation.	No exceptions noted
CC9.0 - Risk Mitigation			
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.	CC9.1.1	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

Description of Company Controls	Criteria Number	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.			
A risk assessment is performed on an annual basis to identify and rank potential threats to the system.	CC9.1.2	Inspected the risk assessment to determine that a risk assessment was completed within a year and identified and ranked potential threats to the system.	No exceptions noted
The company has a defined Business Continuity Plan that outlines the proper procedures to respond, recover, resume, and restore operations following a disruption.	CC9.1.3	Inspected the company's Business Continuity Plan to determine that it defined proper procedures to respond, recover, resume, and restore operations following a disruption.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	CC9.2.1	Inspected the annual vendor review to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	Exception noted: Sensiba observed that evidence of an annual review of critical vendor compliance reports was not available for audit. See management's response to the exception in Section 5.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
The company has a defined vendor management policy that establishes requirements of ensuring third-party entities meet the organization's data preservation and protection requirements.	CC9.2.2	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
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.			
The company has implemented tools to monitor servers and notify appropriate personnel of any events or incidents based on predetermined criteria. Incidents are escalated per policy.	A1.1.1	Inspected 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
A1.2 - 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.			
The company relies on the subservice organization's physical and environmental controls, as defined and tested within the subservice organization's SOC 2 efforts.	A1.2.1	Not Applicable - Control is Carved Out	The Criterion is carved out and the responsibility of the subservice organization.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result
A1.3 - The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
The company performs backups daily and retains them in accordance with a predefined schedule in the Backup Policy.	A1.3.1	Inspected the database configuration to determine that backups are made daily using the infrastructure provider's automated backup service.	No exceptions noted
The company conducts annual BCP/DR tests and documents according to the BCDR Plan.	A1.3.2	Inspected the annual disaster recovery exercise to determine that the Company's disaster recovery plan is tested annually to ensure that recovery procedures are complete and accurate.	No exceptions noted

5. Other Information Provided by Management

The information included in Section 5 of this report is presented by management of Coderbyte to provide additional information to user entities and is not a part of the description of the system. Information included here in Section 5 has not been subjected to the procedures applied in the examination of the description of the system related to description of the system, and accordingly, Sensiba LLP expresses no opinion on it.

Description of Company Controls	Criteria Number	Service Auditor's Test of Controls	Result	Management's Response to Exceptions Noted
The company maintains a directory of its key vendors, including their compliance reports. Critical vendor compliance reports are reviewed annually.	CC9.2.1	Inspected the annual vendor review to determine that security documentation, including SOC 2 reports, are collected from sub-service organizations and key vendors.	Exception noted: Sensiba observed that evidence of an annual review of critical vendor compliance reports was not available for audit.	Management acknowledges the auditor's observation. While the review of critical vendor compliance reports was conducted within a spreadsheet during the audit period, evidence of this activity was not formally retained within our GRC platform. At the time, our GRC tool had limited features to support vendor management processes, which contributed to the absence of centralized documentation. To address this issue, the company is enhancing its vendor management procedures to ensure that all future reviews of critical vendor compliance reports are properly documented and securely retained within our GRC platform. These enhancements include the implementation of a standardized review checklist and the establishment of centralized storage for audit evidence. These measures will help ensure consistent adherence to internal controls and provide verifiable documentation for future audits.