Independent Assurance Report on Coderbyte Enterprise Inc.'s Description of its System and on the Suitability of the Design of its Controls Relevant to Security and Availability Trust Services Criteria (SOC 2)

Prepared in accordance with the following:
AT-C section 105: Concepts Common to All Attestation Engagements
AT-C section 205: Assertion-Based Examination Engagements

assurancelab

CONTENTS

SECTION I –

ASSERTION OF CODERBYTE ENTERPRISE INC. MANAGEMENT

ASSERTION OF CODERBYTE ENTERPRISE INC. MANAGEMENT

November 6, 2023

We have prepared the accompanying description of Coderbyte Enterprise Inc.'s ('Coderbyte') Software as a Service System (the 'Description') for the purposes of the independent assurance report. We have prepared the Description in accordance with the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the Coderbyte Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with Coderbyte's system. This includes the controls that Coderbyte has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/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 (AICPA, Trust Services Criteria).

Coderbyte uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services, and Heroku ('subservice organization') for Platform as a Service ('PaaS'). 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 Agreed Criteria. The Description presents Coderbyte's controls, the Agreed 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 are necessary, along with controls at Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the Agreed Criteria. The Description presents Coderbyte's controls, the Agreed 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 Coderbyte's Software as a Service System that was designed and implemented as of 26 October 2023, in accordance with the Description Criteria; and

b. the controls stated in the Description were suitably designed as of 26 October 2023, to provide reasonable assurance that Coderbyte's service commitments and system requirements would be achieved based on the Agreed Criteria, if the controls operated effectively as of that date, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Coderbyte's controls operated effectively as of that date.

Daniel Borowski
Founder and Chief Executive Officer
Coderbyte Enterprise Inc.

SECTION II –
INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Coderbyte Enterprise Inc.

Scope

We have examined Coderbyte Enterprise Inc.'s ('Coderbyte') accompanying description of its Software as Service System (the 'Description') which has been prepared for the purposes of the independent assurance report.

Coderbyte prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: the criteria for a description of a service organization's system in DC section 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria) with regards to the Description.

The Description is intended to provide report users with information about the Coderbyte Software as a Service System (the 'System') that may be useful when assessing the risks arising from interactions with Coderbyte's system. This includes the controls that Coderbyte has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/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 (AICPA, Trust Services Criteria).

Coderbyte uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services and Heroku ('subservice organization') for Platform as a Service ('PaaS). 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 Agreed Criteria. The complementary subservice organization controls have been reviewed by Coderbyte management. The Description does not disclose the actual controls at the subservice organizations. 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 includes complementary user entity controls that are necessary, along with controls at Coderbyte, to achieve Coderbyte's service commitments and system requirements based on the Agreed Criteria. The Description presents Coderbyte's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Coderbyte's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

Service Organization’s Responsibilities

Coderbyte is responsible for its service commitments and system requirements and for designing and implementing 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 Enterprise Inc. Management” (‘the Assertion’) about the Description and the suitability of the design of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. 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 Agreed Criteria and stating the related controls in the Description; and identifying the risks that threaten the achievement of the Coderbyte’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the Description and on the suitability of the design of controls stated in the Description based on our examination. Our examination was conducted in accordance with AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (AICPA). Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects:

- The Description is presented in accordance with the Description Criteria.
- The controls stated in the Description were suitably designed.

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 Coderbyte’s system and the suitability of the design of controls involves the following:

- Obtaining an understanding of the system and Coderbyte’s service commitments and system requirements.
- Assessing the risks that the Description is not presented in accordance with the Description Criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the Description is presented in accordance with the Description Criteria.
- Performing procedures to obtain evidence about whether controls stated in the Description were suitably designed to provide reasonable assurance that Coderbyte achieved its service commitments and system requirements based on Agreed Criteria.
- Evaluating the overall presentation of the Description.

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 report users may consider important to meet their informational needs.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

1) the Description presents Coderbyte's Software as a Service System that was designed and implemented as of 26 October 2023, in accordance with the Description Criteria; and
2) the controls stated in the Description were suitably designed as of 26 October 2023 to provide reasonable assurance that Coderbyte's service commitments and system requirements would be achieved based on the Agreed Criteria, if its controls operated as of that date and if the subservice organizations and user entities applied the complementary controls assumed in the design of Coderbyte's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Coderbyte, user entities of Coderbyte's Software as a Service System, business partners of Coderbyte subject to risks arising from interactions with the 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 Agreed 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.

Erika Villanueva

Erika Villanueva, CA, CPA
AssuranceLab Pty Ltd
Sydney, Australia
November 6, 2023

SECTION III –

CODERBYTE ENTERPRISE INC.'S DESCRIPTION OF ITS SYSTEM

OVERVIEW OF OPERATIONS

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.

Description of 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.

System	Type	Description
Heroku	Platform as a Service	Enables developers to build, run, and operate applications entirely in the cloud.

System	Type	Description
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.

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.
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.

Software	Purpose
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 that 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.

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.

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 Governance

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.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, INFORMATION AND COMMUNICATION, AND MONITORING

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

Risk Assessments

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 the risks 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 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, 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 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 Common Criteria/Security and Availability Trust Services Criteria were applicable to Coderbyte's Software as a Service System.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by Amazon Web Services ('AWS'), and Heroku.

Subservice Description of Services

AWS

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia.

Heroku

Heroku is a container-based cloud Platform as a Service ('PaaS') that lets companies build, deliver, monitor, and scale applications. The Heroku platform is hosted on Amazon Web Services infrastructure.

Complementary Subservice Organization Controls

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

AWS

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 – Amazon Web Services		
Category	**Criteria**	**Control**
Common Criteria/ 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.
Common Criteria/ Security	CC6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.

Subservice Organization – Amazon Web Services		
Category	**Criteria**	**Control**
		Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
Common Criteria/ 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.
Common Criteria/ 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.
Availability	A1.2	Amazon-owned data centers are protected by fire detection and suppression systems.
		Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels.
		Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon-owned data centers.
		Amazon-owned data centers have generators to provide backup power in case of electrical failure.
		Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies.
		AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards.

Subservice Organization – Amazon Web Services		
Category	**Criteria**	**Control**
		If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery.
		Critical AWS system components are replicated across multiple Availability Zones and backups are maintained.

Heroku

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

Subservice Organization – Heroku		
Category	**Criteria**	**Control**
Common Criteria/ 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.
	CC6.4	Physical access measures are established and followed to ensure access to facilities and protected information assets is restricted to authorized personnel.
	CC6.6 - CC6.8	Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters
		Security groups are configured to restrict access to the production environment.
	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.
	CC7.2	A centralized management tool is utilized to configure and monitor production infrastructure.
	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.

Coderbyte 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, Coderbyte performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

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 Agreed Criteria related to Coderbyte's services to be solely achieved by Coderbyte 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 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 Coderbyte's terms of service.
- Notifying Coderbyte 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.
- Performing any required risk assessments and approvals when using pre-built integrations available with Coderbyte's services.
- Performing any required risk assessments and approvals for using Coderbyte's open application programming interface (API), and notifying Coderbyte of any identified vulnerabilities, security breaches or system failures when using the APIs.
- Ensuring the supervision, management, and control of the use of Coderbyte's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Coderbyte services for any critical reliance on these services.
- Immediately notifying Coderbyte of any actual or suspected information security breaches or system failures.

SOC 2 TRUST SERVICES CRITERIA

Trust Services Categories Selected by Coderbyte

Common Criteria (*to all Categories)*
Security refers to the protection of i. information during its collection or creation, use, processing, transmission, and storage and ii. systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability
Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

SECTION IV –
CRITERIA AND RELATED CONTROLS

SOC 2 TRUST SERVICES CRITERIA

Trust Services Criteria for the Security Category

Common Criteria 1: Control Environment

CC1.0	Criteria	Control Activity
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.
		Background checks are conducted for new hires prior to onboarding.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		The information security policies are communicated, read, and acknowledged by employees.
CC1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Coderbyte's Security Advisory team meets at least quarterly and maintains meeting minutes.
		Coderbyte's Security Advisory team has a documented charter that outlines its oversight responsibilities for internal control and information security.
		The Security Advisory team maintains oversight and provides support for the information security program with briefings at least annually.
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Job descriptions are documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual.
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
		The documented organization chart outlines the roles, functional responsibilities, and reporting lines for Coderbyte personnel.
		Coderbyte's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.

CC1.0	Criteria	Control Activity
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.
		Background checks are conducted for new hires prior to onboarding.
		Coderbyte evaluates the performance of all employees through a formal, annual performance review.
		Security awareness training is conducted for Coderbyte employees at least annually.
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The code of conduct establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment.
		Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization.
		Coderbyte evaluates the performance of all employees through a formal, annual performance review.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		The documented organization chart outlines the roles, functional responsibilities and reporting lines for Coderbyte personnel.

Common Criteria 2: Information and Communication

CC2.0	Criteria	Control Activity
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Information logs related to the information processing activities are centrally stored for retrospective analysis where required.
		The encryption policy establishes the roles, responsibilities, and requirements for securing the network with cryptographic controls and security hardening.
		Coderbyte maintains an architecture diagram to document the system boundaries and support the functioning of internal control.
		The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance.
		The asset management policy establishes Coderbyte's scope of information assets and requirements for how those are tracked and managed accordingly.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		Coderbyte performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are logged and planned where weaknesses or potential improvements are identified.
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 information security policy and responsible disclosure policy define the contacts and methods for employees to report security-related incidents and concerns.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		Security awareness training is conducted for Coderbyte employees at least annually.
		The information security policies are communicated, read, and acknowledged by employees.

CC2.0	Criteria	Control Activity
		The incident response plan defines the roles, responsibilities, and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		Coderbyte's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Terms of service are agreed with Coderbyte's customers and users of the services to communicate their responsibilities and terms of use.
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.
		The incident response plan defines the roles, responsibilities, and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence.
		Coderbyte follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		The vulnerability management program defines the approach to identifying, assessing, and resolving security vulnerabilities, including defined timeframes based on severity.
		The vendor management policy sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.

CC2.0	Criteria	Control Activity
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.

Common Criteria 3: Risk Assessment

CC3.0	Criteria	Control Activity
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The information security policies are reviewed by management at least annually and updated where required.
		The information security policies are communicated, read, and acknowledged by employees.
		Coderbyte has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls, and the risk tolerance.
		Coderbyte's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Coderbyte obtains and reviews the third-party attestations or performs other security and compliance assessments of high-risk vendors.
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.
		Coderbyte's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.
		The vendor management policy sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.
		Coderbyte conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Coderbyte has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls, and the risk tolerance.
CC3.3	COSO Principle 8: The entity considers the potential for fraud in	Coderbyte's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities.

CC3.0	Criteria	Control Activity
	assessing risks to the achievement of objectives.	Coderbyte conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Coderbyte has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls, and the risk tolerance.
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The vendor management policy sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.
		Coderbyte conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
		Coderbyte has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls, and the risk tolerance.
		The documented organization chart outlines the roles, functional responsibilities, and reporting lines for Coderbyte personnel.

Common Criteria 4: Monitoring Activities

CC4.0	Criteria	Control Activity
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and / or separate evaluations to ascertain whether the components of internal control are present and functioning.	Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework.
		Independent penetration tests are conducted annually. Results are reviewed by management and tracked through to resolution.
		Vulnerability scans are conducted on a quarterly basis. Identified vulnerabilities are logged, classified, and tracked through to resolution in a timely manner based on their severity.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
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.	Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework.
		The incident response plan defines the roles, responsibilities, and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Independent penetration tests are conducted annually. Results are reviewed by management and tracked through to resolution.
		Vulnerability scans are conducted on a quarterly basis. Identified vulnerabilities are logged, classified, and tracked through to resolution in a timely manner based on their severity.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		The Security Advisory team maintains oversight and provides support for the information security program with briefings at least annually.

Common Criteria 5: Control Activities

CC5.0	Criteria	Control Activity
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		Coderbyte conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The information security policy and responsible disclosure policy define the contacts and methods for employees to report security-related incidents and concerns.
		The encryption policy establishes the roles, responsibilities, and requirements for securing the network with cryptographic controls and security hardening.
		Security awareness training is conducted for Coderbyte employees at least annually.
		The information security policies are communicated, read, and acknowledged by employees.
		Coderbyte conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		Coderbyte authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.
		Independent penetration tests are conducted annually. Results are reviewed by management and tracked through to resolution.
		Vulnerability scans are conducted on a quarterly basis. Identified vulnerabilities are logged, classified, and tracked through to resolution in a timely manner based on their severity.

CC5.0	Criteria	Control Activity
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		Coderbyte conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions.
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 information security policies are reviewed by management at least annually and updated where required.
		The information security policies are communicated, read, and acknowledged by employees.
		Coderbyte's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives.

Common Criteria 6: Logical and Physical Access Controls

CC6.0	Criteria	Control Activity
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	User accounts are individually assigned with a unique user ID to support system logging and accountability.
		Coderbyte has established formal guidelines for passwords to govern the management and use of authentication mechanisms.
		Multi-factor authentication is required for access to sensitive systems.
		The access control policy requires role-based access control where access rights are limited to the requirements of each role.
		The password policy and data protection policy establish the requirements for authentication including strong passwords, multi-factor and single-sign on as applicable to Coderbyte's systems.
		Coderbyte stores sensitive data, including customer data, in databases that are encrypted at rest.
		Coderbyte's workstations have hard-disk encryption applied to protect locally stored data and access credentials.
		Coderbyte employees utilize a password manager to support quality passwords and secure authentication practices.
		The information security policies are reviewed by management at least annually and updated where required.
		The information security policies are communicated, read, and acknowledged by employees.
		The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance.
		The asset management policy establishes Coderbyte's scope of information assets and requirements for how those are tracked and managed accordingly.

CC6.0	Criteria	Control Activity
		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.
CC6.2	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.	User accounts are individually assigned with a unique user ID to support system logging and accountability.
		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.
		A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.
		Coderbyte authorizes access to information resources, including data and the systems that store or process customer data, based on the principle of least privilege.
		The access control policy requires appropriate access approvals, quarterly user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorized personnel.
		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.
CC6.3	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.	User accounts are individually assigned with a unique user ID to support system logging and accountability.
		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.
		The access control policy requires role-based access control where access rights are limited to the requirements of each role.

CC6.0	Criteria	Control Activity
		A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner.
		Quarterly reviews of Coderbyte's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.
		The access control policy requires appropriate access approvals, quarterly user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorized personnel.
		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.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization.
CC6.5	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 in a timely manner.
		The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance.
		The asset management policy establishes Coderbyte's scope of information assets and requirements for how those are tracked and managed accordingly.
		Quarterly reviews of Coderbyte's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required.

CC6.0	Criteria	Control Activity
		The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed.
		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.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	A web application firewall configuration is used to protect Coderbyte's application from unauthorized access and external threats.
		Coderbyte uses firewall configurations that ensure only approved networking ports and protocols can be used.
		Access to cloud data storage is configured to restrict public access.
		The password policy and data protection policy establish the requirements for authentication including strong passwords, multi-factor, and single sign on as applicable to Coderbyte's systems.
		Connections and data flows to Software as a Service system and the supporting infrastructure are encrypted in transit.
		Coderbyte workstations apply screen lock with a timeout of no more than 15 minutes to prevent unauthorized viewing or access.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		Security awareness training is conducted for Coderbyte employees at least annually.
		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	Control Activity
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.	Connections and data flows to Software as a Service system and the supporting infrastructure are encrypted in transit.
		Coderbyte stores sensitive data, including customer data, in databases that are encrypted at rest.
		Coderbyte's workstations have hard-disk encryption applied to protect locally stored data and access credentials.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		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 unauthorized or malicious software to meet the entity's objectives.	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		The encryption policy establishes the roles, responsibilities, and requirements for securing the network with cryptographic controls and security hardening.
		Coderbyte's workstations operating system security patches are applied automatically.
		Antivirus software is installed on workstations to protect against malware.
		The acceptable use policy establishes the boundaries and requirements for how employees use Coderbyte's systems and information assets to protect against data leakage, malware, and security breaches.
		Security awareness training is conducted for Coderbyte employees at least annually.
		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	Control Activity
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		When Coderbyte's application code changes, code reviews and tests are performed by a senior member of the DevOps team prior to production release.
		Coderbyte uses a version control system to manage source code, documentation, release labelling, and other change management tasks. Access to the system must be approved by a system admin.
		Independent penetration tests are conducted annually. Results are reviewed by management and tracked through to resolution.
		Vulnerability scans are conducted on a quarterly basis. Identified vulnerabilities are logged, classified, and tracked through to resolution in a timely manner based on their severity.
		Coderbyte conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time.
		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.
CC7.2	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.	Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework.
		Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity.
		Coderbyte uses logging software that sends alerts to appropriate personnel.
		Information logs related to the information processing activities are centrally stored for retrospective analysis where required.

CC7.0	Criteria	Control Activity
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified, and followed through to resolution in a timely manner based on their severity.
		Independent penetration tests are conducted annually. Results are reviewed by management and tracked through to resolution.
		Vulnerability scans are conducted on a quarterly basis. Identified vulnerabilities are logged, classified, and tracked through to resolution in a timely manner based on their severity.
		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.
CC7.3	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 plan defines the roles, responsibilities, and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Coderbyte has appointed an emergency response team to mobilize and manage incidents through to resolution.
		Coderbyte follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified, and followed through to resolution in a timely manner based on their severity.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		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**	**Control Activity**
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 plan defines the roles, responsibilities, and requirements for identifying, classifying and resolving incidents, including devising lessons learned to prevent recurrence.
		Coderbyte has appointed an emergency response team to mobilize and manage incidents through to resolution.
		Coderbyte follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		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.	Daily backups are performed and monitored to support recoverability of the production data.
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.
		Vulnerabilities identified from the penetration tests, vulnerability scans, and any other sources, are centrally logged, classified, and followed through to resolution in a timely manner based on their severity.
		The business continuity plans document the scenarios and relevant impacts that may threaten Coderbyte's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.

CC7.0	Criteria	Control Activity
		The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents.
		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	Control Activity
CC8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Separate environments are used for testing and production for Coderbyte's Software as a Service system.
		Only authorized Coderbyte personnel can deploy changes into production.
		When Coderbyte's application code changes, code reviews and tests are performed by a senior member of the DevOps team prior to production release.
		Coderbyte uses a version control system to manage source code, documentation, release labelling, and other change management tasks. Access to the system must be approved by a system admin.
		The software development life cycle policy governs the software development lifecycle including tracking, testing, approving and validating changes to the source code.
		Change releases are independently reviewed and approved prior to production release.
		Change releases are tested and approved prior to implementation in production.
		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	Control Activity
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Daily backups are performed and monitored to support recoverability of the production data.
		Coderbyte follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence.
		Coderbyte utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
		Coderbyte conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.
		The backup policy establishes the requirements for backups and recoverability.
		The business continuity plans document the scenarios and relevant impacts that may threaten Coderbyte's continuity, as well as the roles, responsibilities, and plans to manage those events effectively.
		Established incident response plans document the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively.
		Coderbyte maintains cybersecurity insurance to mitigate the impact of potential data breaches and disruptions.
		Restoration tests are conducted to check the integrity and completeness of back-up information on at least an annual basis.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Coderbyte obtains and reviews the third-party attestations or performs other security and compliance assessments of high-risk vendors.

CC9.0	Criteria	Control Activity
		The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities.
		The vendor management policy sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers.

Trust Services Criteria for the Availability Category

A1.0	**Criteria**	**Control Activity**
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.	Auto-scaling configuration is used to automatically provision additional capacity when predefined thresholds are met.
		A load balancer automatically distributes incoming application traffic across multiple instances and availability zones.
		Coderbyte utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.	Daily backups are performed and monitored to support recoverability of the production data.
		Coderbyte utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives.
		Coderbyte conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems.
		The backup policy establishes the requirements for backups and recoverability.
		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.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Daily backups are performed and monitored to support recoverability of the production data.
		Coderbyte conducts annual business continuity and disaster recovery tests to ensure the response plans are effective.
		Restoration tests are conducted to check the integrity and completeness of back-up information on at least an annual basis.

GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR

AssuranceLab's examination of the controls of Coderbyte was limited to the related Agreed Criteria and control activities specified by the management of Coderbyte and did not encompass all aspects of Coderbyte's operations or operations at user entities. Our examination was performed in accordance with AT-C section 105: Concepts Common to All Attestation Engagements and AT-C section 205: Assertion-Based Examination Engagements.

Our examination of the control activities was performed using the following testing methods:

TEST	DESCRIPTION
Inquiry	The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information.
Observation	The service auditor observed application of the control activities by client personnel.
Inspection	The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities.
Re-performance	The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control.

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the Agreed Criteria
- Understand the infrastructure, software, procedures and data that are designed, implemented and operated by the service organization
- Determine whether the Agreed Criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the Agreed Criteria

assurancelab