ConstellationGRC

System and Organization Controls Report (SOC 2® TYPE 1)

Report on CoGrader Co.’s Description of Its Services System and on the Suitability of the Design of Its Controls Relevant to Security as of Jan 27, 2025

cograder

TABLE OF CONTENTS

Section 1: Independent Service Auditor's Report

INDEPENDENT SERVICE AUDITOR'S REPORT

To: CoGrader, Co.

Scope

We have examined CoGrader Labs, Inc.'s ("CoGrader," "Company," "Entity" or "the Service Organization") description of its Services System found in Section 3 titled "System Description " as of January 27, 2025 ("description") based on the criteria for a description of a service organization's system set forth in DC 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 as of January 27, 2025, to provide reasonable assurance that CoGrader's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria.

CoGrader uses Google Cloud Platform (GCP) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoGrader, to achieve CoGrader's service commitments and system requirements based on the applicable trust services criteria. The description presents CoGrader's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of CoGrader's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

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

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

In Section 2, CoGrader has provided the accompanying assertion titled “CoGrader Inc.’s Management Assertion” (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. CoGrader is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor’s Responsibilities

Our responsibility is to express an opinion on the description and the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. 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 a description of a service organization’s system and the suitability of the design of controls involves—

- 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.
- 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 meet our other ethical responsibilities in accordance with ethical requirements relating to the examination 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 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. 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 or 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.

Other Matter

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

Opinion

In our opinion, in all material respects,

- the description fairly presents CoGrader's Services System that was designed and implemented as of January 27, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of January 27, 2025, to provide reasonable assurance that CoGrader's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of CoGrader's controls throughout that period.

Restricted Use

This report is intended solely for the information and use of CoGrader, user entities of CoGrader's Services System as of January 27, 2025, and business partners of CoGrader subject to risks arising from interactions with the Services 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, 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 the specified parties.

Tineyi Gwariwa (Jan 29, 2025 19:36 PST)

Tineyi Gwariwa, CPA, ACA, MSA, MBA
Lakewood Associates P.C.
4217 N Bellflower Blvd
Long Beach CA 90808

Section 2: Cograder's Management Assertion

CoGrader’S Management Assertion

We have prepared the description of CoGrader, Inc.’s (‘CoGrader’ or ‘the Service Organization’) Services System entitled “System Description (Section 3 as of January 27, 2025 (“description”) based on the criteria for a description of a service organization’s system set forth in *DC 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 Cybersecurity Services System that may be useful when assessing the risks arising from interactions with CoGrader’s system, particularly information about system controls that CoGrader has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022) in AICPA, Trust Services Criteria*.

CoGrader uses Google Cloud Platform (GCP) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at CoGrader, to achieve CoGrader’s service commitments and system requirements based on the applicable trust services criteria. The description presents CoGrader’s controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of CoGrader’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 CoGrader, to achieve CoGrader’s service commitments and system requirements based on the applicable trust services criteria. The description presents the subservice organization controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of CoGrader’s controls.

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

- the description presents CoGrader’s Services System that was designed and implemented as of January 27, 2025, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of January 27, 2025, to provide reasonable assurance that CoGrader’s service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of CoGrader’s controls.

CoGrader,. Co..

Jan 27, 2025

Section 3: CoGrader’S Description of its Services System

CoGrader System Description

Company Overview

CoGrader, founded in and headquartered in New York, NY US, is a SaaS company that provides AI models for educational grading services. It serves individual educators.

System Description

The system in-scope for this report is the CoGrader software hosted on Google Cloud Platform. The CoGrader Platform offers Artificial Intelligence for educators seeking more efficient grading solutions. Specifically, it provides the following service of CoGrader AI Essay Grader.

System Boundaries

The scope of this report includes CoGrader Platform and the supporting production systems, infrastructure, software, people, data and policies and procedures. The following service is in-scope for this report: CoGrader AI Essay Grader.

Subservice Organizations

CoGrader uses multiple subservice organizations as described in the “Subservice Organizations” section below, including Google Cloud Platform. The subservice organizations are excluded from the scope of this report.

A. Principal Service Commitments and System Requirements

CoGrader structures its processes and procedures to meet its objectives, which are based on service commitments to users, relevant laws and regulations, and the financial, operational, and compliance standards established for its services. The system adheres to Security commitments as outlined in service agreements and other customer contracts, which consist of the following:

- All databases are encrypted at rest, and data in transit is secured using Transport Layer Security (TLS) or equivalent technologies over public networks.
- The company enforces the principle of least privilege for identity and access management, ensuring team members only access the data necessary for their roles.
- A minimum password complexity is enforced, with multi-factor authentication (MFA) implemented wherever possible to strengthen access security.
- Company-provided workstations are protected with security protocols like full-disk encryption, screen locks, and strong password policies.
- Firewalls are used to safeguard against potential attacks.

- Employees are required to undergo regular security awareness training covering industry best practices, phishing prevention, and password management.
- All new hires undergo background checks in accordance with local laws to verify trustworthiness.
- Routine vulnerability scans are performed, and active threat monitoring helps detect and mitigate potential risks.
- A defined incident management process includes escalation procedures, rapid mitigation, and timely communication in the event of a security breach.
- Thorough risk assessments and reviews are conducted before onboarding new vendors to ensure they meet security standards.
- The company conducts annual risk assessments to identify potential threats, including those related to fraud.

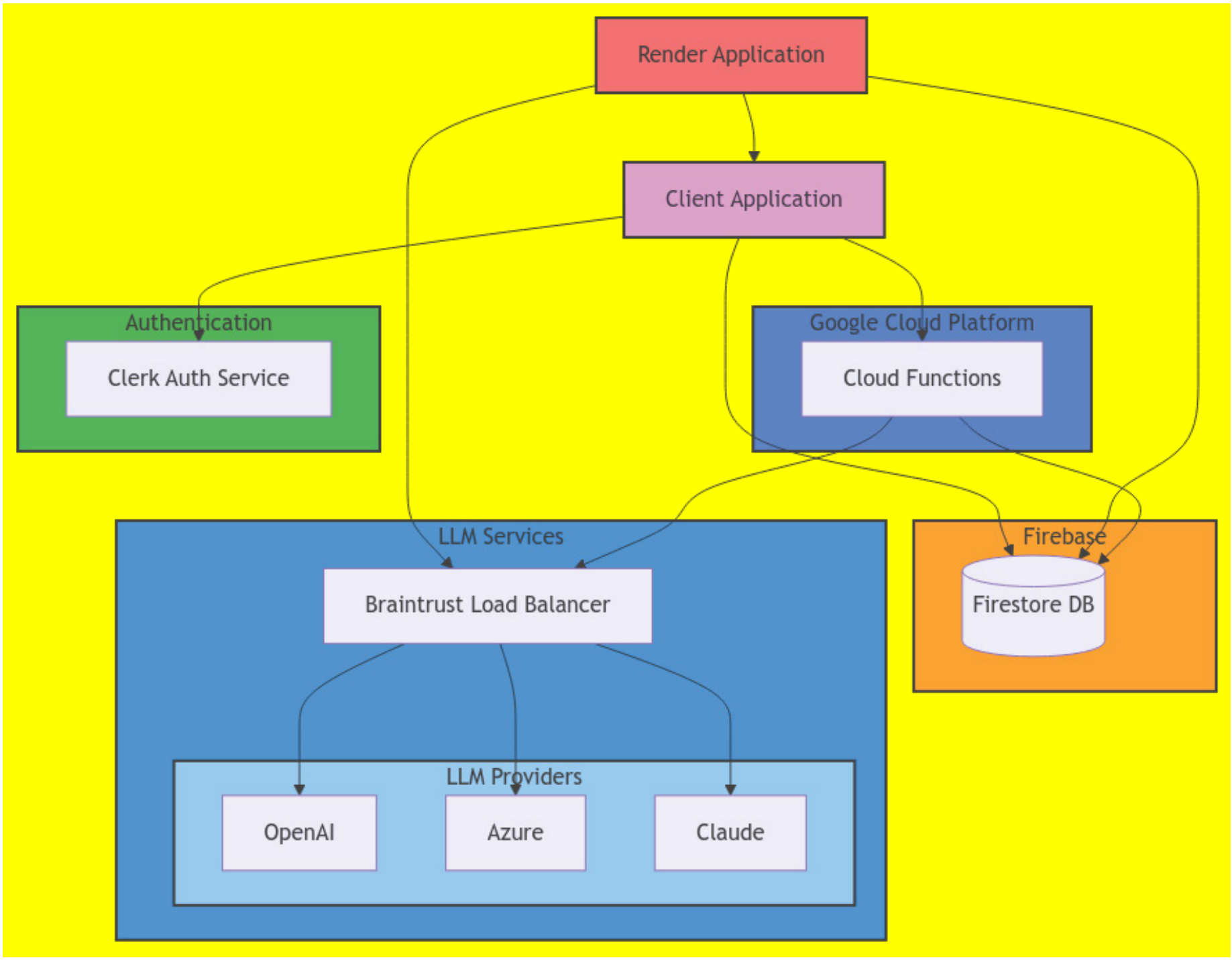
B. System Components

Infrastructure

The CoGrader's CoGrader Platform is comprised of the following components:

Hardware	Type	Purpose
Web Servers	GCP	Host Application
Database	Firebase Firestore DB	Store Customer Data
Large Language Model	OpenAI, Azure, Claude	Process and produce natural language for generative AI

The CoGrader Platform's components operate according to the following network diagram:



Software

CoGrader utilizes the following software to support CoGrader Platform:

Software	**Purpose**
Close.io	*CRM Platform*
Customer.io	*CRM Platform*
Posthog	*Feature testing*
GitHub	*Source code and development projects tool*
Google Workspace	*Identity Provider*
Google Cloud Platform	*Cloud Provider*

Deel	*Payroll System*
Slack	*Workplace collaboration tool*

Data

Data is classified in accordance with the written Data Management Policy, including the following:

- Confidential Data,
- Restricted Data,
- Internal Data, and
- Public Data.

Public data is information that may be disclosed to any person regardless of their affiliation with CoGrader.

Internal data is information that is potentially sensitive and is not intended to be shared with the public.

Confidential data is information that, if made available to unauthorized parties, may adversely affect individuals or CoGrader.

Restricted data includes any information that CoGrader has a contractual, legal, or regulatory obligation to safeguard in the most stringent manner.

Data is ingested into the system through manual uploads and Automated APIs. Data is stored in Firebase Firestore DB. The databases are all encrypted at rest using AES-256. The Company uses TLS 1.2 to encrypt data during transmission across public networks. Access to all relevant cloud resources that hold customer data or support production infrastructure is restricted, requiring documented approval from appropriate personnel before any access is granted.

People

CoGrader has 4 employees organized in the following functional areas:

- **Management:** Oversees employee performance & maintains security and compliance across the organization:
  CEO -Gil Flores
  CTO / Head of Engineering -Vitor Barbosa
  COO / Head of Operations -Gabriel Adamante

- **Engineering & Product Development**: Develops and designs our software product.

Policies and procedures

CoGrader's policies and procedures ensure its security, availability, and confidentiality. All personnel accept and observe CoGrader's policies and procedures, including:

- Code of Conduct
- Information Security Policy
- Information Security Roles and Responsibilities
- System Operations Security Policy
- Incident Response Policy
- Business Continuity & Disaster Recovery Plan
- Secure Development Policy
- Asset Management Policy
- Data Management Policy
- Access Control Policy
- Human Resources Policy
- Physical Security Policy
- Risk Management Policy
- Vendor Management Policy
- Encryption Policy

C. Relevant Aspects Of The Control Environment, Risk Assessment Process, Information And Communication, And Monitoring

Control Environment

The internal control environment demonstrates the commitment and approach of executive management and key stakeholders toward the importance of controls, emphasizing their role within the company's policies and procedures.

Integrity and Ethical Values

Management oversees operations, ensuring the establishment, communication, and enforcement of policies and procedures. A key responsibility includes maintaining strong internal controls and fostering a culture of integrity and ethical behavior among personnel.

As part of the hiring process, background checks on employees are conducted to ensure the company's standards are upheld.

During onboarding, new employees undergo security and privacy training, and they review and acknowledge company policies, including the Code of Conduct.

Governance and Structure

Senior management meets annually to discuss business goals, initiatives, resource needs, risk management, and other relevant internal or external matters.

Management maintains an official organizational chart to clearly define authority and communication lines, distributing it to internal personnel via a Slack channel. Additionally, roles and responsibilities, particularly those related to security, are outlined in job descriptions and the IT Roles and Responsibilities policy.

Access Control

CoGrader follows the principle of least privilege, granting users only the minimum necessary access based on their role. Access to production systems and databases is tightly controlled, with only senior management and engineers given elevated access where essential for their duties. User access is protected by secure login methods that include unique usernames, strong passwords, and multi-factor authentication (MFA).

Access activities are continuously monitored and periodically reviewed based on employees' roles and responsibilities.

When onboarding new employees, access levels are reviewed and assigned based on their role. Offboarding involves promptly revoking access within 24 hours, and collecting company-issued devices. Both employee onboarding and offboarding are documented through a checklist, and tracked via internal ticketing systems.

Change Management

Changes to applications or infrastructure follow a documented process as outlined in the Change Management Policy & Secure Development Policy. All changes are tracked, with quality assurance testing and code reviews performed in a separate environment before pushing to production

Source code is managed in a private GitHub repository, with version control allowing for tracking changes and rollbacks as needed.

Network Security

Firewalls are implemented to filter and block unauthorized inbound traffic from the internet, permitting only explicitly authorized connections. Administrative access to firewall configurations is limited to authorized personnel.

Physical Security

The in-scope system infrastructure is hosted by Google Cloud Platform. Hence, Google Cloud Platform. is responsible for physical security of the infrastructure. More details can be found in the "Subservice Organizations" section.

Vulnerability Management

Vulnerability scans are conducted regularly, and critical patches are applied following a structured review process. Annual penetration tests are performed to assess security risks.

Incident Response and Business Continuity

Incident response procedures are in place to handle any security events or breaches. The Company utilizes various methods to detect potential security incidents, and confirmed incidents are documented and tracked in accordance with the Security Incident Response Plan. The Security Incident Response Plan undergoes annual testing to evaluate its effectiveness, with management making modifications based on the test outcomes. To ensure business continuity in the event of a disaster or third-party attack, the company maintains backups of production data.

Customer data is configured to be automatically backed up daily in Google Cloud Platform., with backups encrypted at rest. The CTO monitors the backup process for successful completion and any exceptions. In case of an issue, they troubleshoot the root cause and either rerun the backup or address it during the next scheduled backup.

Risk Assessment Process

CoGrader has implemented a risk management procedure to evaluate both information security and business risks. A formal risk assessment is conducted and documented in a risk register annually to identify, assess, and update threats related to security, including the risk of fraud. The risk register also tracks risk mitigation strategies and any modifications to controls in line with these strategies.

Given CoGrader's reliance on external vendors for critical operations and infrastructure, a Vendor Management Policy has been established. This policy outlines security standards for vendors, as well as the company's due diligence and monitoring responsibilities. CoGrader’s vendor agreements include specific security requirements, and the company reviews compliance reports such as SOC 2 or ISO 27001 at least annually for high-risk vendors.

Information and Communication

To support CoGrader's business goals and ensure operational performance, management fosters effective communication with both internal and external stakeholders.

Internal Communications

Information exchange within CoGrader is a vital part of the internal control system, ensuring that critical information is identified, processed, and shared promptly. Employees are required to report any security incidents, operational disruptions, or system issues as part of their responsibility to maintain the security and smooth functioning of operations. Security leadership and document owners review and approve security policies and procedures annually to ensure they align with current risks and requirements.

When significant changes are made to policies or procedures, they are communicated internally to ensure all team members are informed and can implement the necessary updates.

External Communications

To promote transparency, CoGrader publishes details of its services and security commitments on its website. Customers can access support and report security concerns via the platform in a support ticket, and these communications are monitored in accordance with the Security Incident Response Plan. System changes, incidents, or unauthorized disclosures are communicated following the guidelines set out in the Change Management Policy and Security Incident Response Plan.

Customer commitments & responsibilities are communicated through CoGrader's Terms of Service (https://cograder.com/terms-and-conditions).

Monitoring Controls

CoGrader employs various monitoring methods to evaluate the security and health of the in-scope environment and its related controls. The company utilizes a continuous monitoring solution that assesses internal controls in relation to service commitments and system requirements, identifying non-compliance issues for management to address.

Logging is activated, and monitoring tools are set up to gather metrics from ingested logs, which help detect potential security threats, unusual system behavior, and monitor overall system performance as needed. Security leadership meets quarterly to align on security initiatives, review network security, manage infrastructure, and discuss security risks.

D. Trust Services Criteria and Related Controls

Although the applicable trust services criteria and related controls are presented in Section IV of this report, they are an integral part of CoGrader's system description.

E. Subservice Organizations

The Company engages the subservice organizations in the tables below to achieve its objectives.

To effectively monitor the services provided by these organizations, the Company implemented the following controls: collect and review compliance reports (SOC 2, ISO 27001 or equivalent security due diligence documentation) for its high-risk vendors at least annually.

Complementary Subservice Organization Controls	Criteria

Google Cloud Platform. The subservice organization hosts the Company's cloud infrastructure. This organization was excluded from the scope of this report.	
1 Conducts periodic vulnerability assessments.	CC 3.2
2 Data centers are safeguarded by fire detection and suppression systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators.	CC 5.2
3 System changes to customer-impacting aspects of a service are reviewed, tested and approved before merging to production.	CC 5.2, CC 8.1
4 Maintains contingency planning and incident response procedures to reflect emerging continuity risks and lessons learned from past incidents	CC 5.2, CC 7.4, CC 7.5
5 User logical access is approved by appropriate personnel, is reviewed periodically, and is revoked upon termination of the individual.	CC 6.1, CC 6.2, CC 6.3, CC 6.6
6 Customer data is encrypted with strong encryption keys, and encryption keys are logically secured.	CC 6.1
7 User logical access modifications are approved by appropriate personnel prior to being provisioned.	CC 6.3
8 Physical access to the data centers is approved by authorized personnel, is reviewed periodically, and is revoked upon termination of the individual.	CC 6.4
9 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.	CC6.5
10 Data is encrypted in transit.	CC 6.6, CC 6.7
11 implemented monitoring to identify and notify personnel of potential issues and/or incidents.	CC 7.1, CC 7.5
12 Implements incident response procedures to identify, track, and respond to incidents.	CC 7.3, CC 7.4, CC 7.5
13 Customer data is not used in test and development environments.	CC 8.1
14 Maintains a formal risk management program to continually identify, assess and resolve information security risks that impact business objectives, regulatory requirements, and customers.	CC 9.2

Complementary Subservice Organization Controls	Criteria
GitHub The subservice organization provides the Company with cloud-based source control software. This organization was excluded from the scope of this report.	
1 Conducts periodic vulnerability assessments.	CC 3.2
Data centers are safeguarded by fire detection and suppression 2 systems, air conditioning systems, uninterruptible power supply (UPS) units, and backup generators.	CC 5.2
System changes to customer-impacting aspects of a service 3 are reviewed, tested and approved before merging to production.	CC 5.2, CC 8.1
Maintains contingency planning and incident response 4 procedures to reflect emerging continuity risks and lessons learned from past incidents	CC 5.2, CC 7.4, CC 7.5
User logical access is approved by appropriate personnel, is 5 reviewed periodically, and is revoked upon termination of the individual.	CC 6.1, CC 6.2, CC 6.3, CC 6.6
6 Customer data is encrypted with strong encryption keys, and encryption keys are logically secured.	CC 6.1
7 User logical access modifications are approved by appropriate personnel prior to being provisioned.	CC 6.3
Physical access to the data centers is approved by authorized 8 personnel, is reviewed periodically, and is revoked upon termination of the individual.	CC 6.4
Discontinues logical and physical protections over physical assets only after the ability to read or recover data and software 9 from those assets has been diminished and is no longer required.	CC6.5
10 Data is encrypted in transit.	CC 6.6, CC 6.7
11 implemented monitoring to identify and notify personnel of potential issues and/or incidents.	CC 7.1, CC 7.5
12 Implements incident response procedures to identify, track, and respond to incidents.	CC 7.3, CC 7.4, CC 7.5
13 Customer data is not used in test and development environments.	CC 8.1
Maintains a formal risk management program to continually identify, assess and resolve information security risks that 14 impact business objectives, regulatory requirements, and customers.	CC 9.2

F. Complementary User Entity Controls

To provide reasonable assurance that CoGrader's service commitments and system requirements are achieved based on the applicable trust services criteria, user entities utilizing CoGrader Platform are expected to implement specific controls. Each user entity should evaluate its internal control environment to determine if the following controls are in place:

Control Responsibilities to be Considered by User Entities	Criteria
1 User entities are responsible for complying with CoGrader's Terms of Service.	CC 2.3
2 User entities are responsible for ensuring that application password settings align with the entity's password policy.	CC 6.1
User entities are responsible for managing their employees' 3 access, ensuring that access is properly approved before being granted and revoked when users are no longer authorized.	CC 6.1, CC 6.2, CC 6.3, CC 6.6
4 User entities are responsible for periodically reviewing access to the CoGrader's application.	CC 6.4
5 User entities are responsible for ensuring the integrity, accuracy and completeness of the data entered into CoGrader Platform.	CC 6.7
6 User entities are responsible for promptly informing CoGrader of any confirmed or suspected information security incidents.	CC 7.1, CC 7.2

Section 4: CoGrader’S Controls

Trust Services Category, Criteria, and Related Controls

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design of controls to meet the criteria for the Security, Availability and Confidentiality categories set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus – 2022)* in AICPA, Trust Services Criteria as of January 27, 2025.

The trust services category for the Security, Availability and Confidentiality criteria and related controls specified by CoGrader are presented in the below tables.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

CC1.0 – Common Criteria Related to the Control Environment

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values	**CA-01** - The company requires contractor agreements to include a code of conduct or reference to the company code of conduct. **CA-02** - The company requires contractors to sign a confidentiality agreement at the time of engagement. **CA-03** - The company requires employees to sign a confidentiality agreement during onboarding. **CA-04** - The company performs background checks on new employees. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-06** - The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	**CA-07** - The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. **CA-08** - The company's board of directors meets at least annually and maintains formal meeting minutes. **CA-09** - The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed. **CA-10** - The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	**CA-10** - The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control. **CA-11** - The company maintains an organizational chart that describes the organizational structure and reporting lines. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-13** - The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	**CA-04** - The company performs background checks on new employees. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-14** - The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
CC 1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	**CA-01** - The company requires contractor agreements to include a code of conduct or reference to the company code of conduct. **CA-05** - The company managers are required to complete performance evaluations for direct reports at least annually. **CA-06** - The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy. **CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-17** - The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	**CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-13** - The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls. **CA-14** - The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter. **CA-18** - The company communicates system changes to authorized internal users. **CA-19** - The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns. **CA-20** - The company provides a description of its products and services to internal and external users. **CA-21 -** The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-22** - The company's information security policies and procedures are documented and reviewed at least annually.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	**CA-04** - The company performs background checks on new employees. **CA-23** - The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS). **CA-24** - The company provides guidelines and technical support resources relating to system operations to customers. **CA-25** - The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel. **CA-26** - The company notifies customers of critical system changes that may affect their processing. **CA-27** - The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-29** - The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually. **CA-32** - The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC 3.4- COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	**CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-33** - The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. **CA-34** - The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually. **CA-33** - The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	**CA-15** - The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	**CA-22** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies.
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	**CA-22** - The company's information security policies and procedures are documented and reviewed at least annually. **CA-35** - The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access.
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	**CA-12** - Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy. **CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-29** - The company specifies its objectives to enable the identification and assessment of risk related to the objectives. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-37** - The company specifies its objectives to enable the identification and assessment of risk related to the objectives. **CA-38** - The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-40** - The company's data backup policy documents requirements for backup and recovery of customer data.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC6.1 - The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-41** - The company's datastores housing sensitive customer data are encrypted at rest. **CA-42** - The company restricts privileged access to encryption keys to authorized users with a business need. **CA-43** - The company restricts privileged access to the firewall to authorized users with a business need. **CA-44** - The company's network is segmented to prevent unauthorized access to customer data. **CA-45** - The company requires passwords for in-scope system components to be configured according to the company's policy. **CA-46** - The company requires authentication to the “production network” to use unique username and password or authorized Secure Socket Shell (SSH) keys. **CA-47** - The company restricts privileged access to databases to authorized users with a business need. **CA-48** - The company maintains a formal inventory of production system assets. **CA-49** - The company restricts privileged access to the production network to authorized users with a business need. **CA-50** - The company restricts privileged access to the operating system to authorized users with a business need. **CA-51** - The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-53** - The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys. **CA-54** - The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. **CA-55** - The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. **CA-56** - The company restricts access to migrate changes to production to authorized personnel. **CA-57** - The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel. **CA-58** - System access restricted to authorized access only.
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-46** - The company requires authentication to the “production network” to use unique username and password or authorized Secure Socket Shell (SSH) keys. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-59** - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	**CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-46** - The company requires authentication to the "production network" to use unique username and password or authorized Secure Socket Shell (SSH) keys. **CA-52** - The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned. **CA-59** - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data centre facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	**CA-59** - The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion. **CA-61** - The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners. **CA-62** - The company reviews access to data centers at least annually. **CA-63** - The company requires visitors to sign-in, wear a visitor badge, and be escorted by an authorized employee when accessing the data center or secure areas.
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	**CA-38** - The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data. **CA-64** - The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed. **CA-65** - The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	**CA-46** - The company requires authentication to the “production network” to use unique username and password or authorized Secure Socket Shell (SSH) keys. **CA-54** - The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection. **CA-55** - The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method. **CA-66** - The company uses firewalls and configures them to prevent unauthorized access. **CA-67** - The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. **CA-68** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-69** - The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. **CA-70** - The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually. **CA-71** - The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity’s objectives.	**CA-67** - The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks. **CA-72** - The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service. **CA-73** - The company encrypts portable and removable media devices when used.
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.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-74** - The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-34** - The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment. **CA-36** - The company's access control policy documents the requirements for the following access control functions including adding new users; modifying users; and/or removing an existing user's access. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-75** - The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2 - The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-17** - The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives. **CA-33** - The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-68** - The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches. **CA-75** - The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring. **CA-76** - An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC7.3 - The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	**CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-77** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-77** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. **CA-78** - The company tests their incident response plan at least annually.
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.	**CA-22** - The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users. **CA-32** - The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually. **CA-77** - The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures. **CA-78** - The company tests their incident response plan at least annually.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-33** - The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs. **CA-35** - The company has a formal systems development life cycle methodology in place that governs the development, acquisition, implementation, changes, and maintenance of information systems and related technology requirements. **CA-39** - The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment. **CA-56** - The company restricts access to migrate changes to production to authorized personnel. **CA-67** - The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats. **CA-70** - The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.

CC9.0 – Common Criteria Related to Risk Mitigation

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY	
CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	**CA-16** - Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation. **CA-28** - The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies. **CA-30** - The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives. **CA-79** - The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.	**CA-27** - The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity. **CA-31** - The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.