SOC 2 Type 1 Report

Security Innovation

August 3, 2023

A Type 1 Independent Service Auditor's Report on Controls Relevant to Security and Availability

AUDIT AND ATTESTATION BY

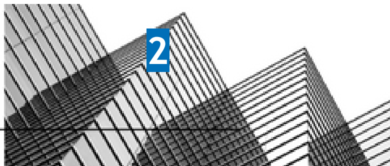
PRESCIENT ASSURANCE

CPA

Prescient Assurance LLC.
1100 Market Street Suite 600
Chattanooga, TN 37402

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents



SECTION 1

Management's Assertion

Management's Assertion

We have prepared the accompanying description of Security Innovation's CMD+CTRL/Basecamp and US Courts Kiosk Systems as of July 17, 2023, 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. The description is intended to provide report users with information about Security Innovation's system that may be useful when assessing the risks arising from interactions with Security Innovation's system, particularly information about system controls that Security Innovation has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Security Innovation uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Security Innovation, to achieve Security Innovation's service commitments and system requirements based on the applicable trust services criteria. The description presents Security Innovation's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Security Innovation's controls. The description does not disclose the actual controls at the subservice organization.

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

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

A. The description presents Security Innovation's system that was designed as of July 17, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of July 17, 2023, to provide reasonable assurance that Security Innovation'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 Security Innovation's controls as of that date.

DocuSigned by:

Jeff Emig

C2ED226BE9C04D7...

Jeff Emig

COO of Security Innovation

SECTION 2

Independent Service Auditor's Report

PRESCIENT

ASSURANCE

Independent Service Auditor's Report

To: Security Innovation

Scope

We have examined Security Innovation's ("Security Innovation") accompanying description of its system as of July 17, 2023, 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, and the suitability of the design of controls stated in the description as of July 17, 2023, to provide reasonable assurance that Security Innovation's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Security Innovation uses a subservice organization for cloud hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Security Innovation, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Security Innovation's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Security Innovation'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 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 Security Innovation, to achieve Security Innovation's service commitments and system requirements based on the applicable trust services criteria. The description presents Security Innovation's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Security Innovation's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service Organization's Responsibilities

Security Innovation 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 Security Innovation's service commitments and system requirements were achieved. In Section 1, Security Innovation has provided the accompanying assertion titled "Management's Assertion of Security Innovation" (assertion) about the description and the suitability of design of controls stated therein. Security Innovation 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 on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements.
2. Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
4. Performing procedures to obtain evidence about whether controls stated in the description were suitably designed and implemented to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Evaluating the overall presentation of the description.

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

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

A. The description presents Security Innovation's system that was designed as of July 17, 2023 in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of July 17, 2023, to provide reasonable assurance that Security Innovation'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 Security Innovation's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Security Innovation, user entities of Security Innovation's system as of July 17, 2023, business partners of Security Innovation 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:

1. The nature of the service provided by the service organization.
2. How the service organization's system interacts with user entities, business partners, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. 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.

Prescient Assurance LLC

DocuSigned by:
John D Wallace
F5ADFA3569EA450...

John D. Wallace, CPA
Chattanooga, TN
August 3, 2023

SECTION 3

System Description

DC 1: Company Overview and Types of Products and Services Provided

Founded in 2002, Security Innovation has established its presence in Seattle, Washington, Wilmington, Massachusetts, and Pune, India. As a renowned worldwide leader in cybersecurity training and advisory solutions, our mission is to enable organizations to proactively handle and reduce cyber threats. Our dedication lies in fostering education, creativity, and cooperation to construct a protected digital landscape for businesses, governments, and individuals across the globe.

At Security Innovation, we understand that cybersecurity is an ongoing battle in an ever-evolving threat landscape. Our mission is to equip organizations with the knowledge, skills, and tools necessary to safeguard their digital assets and protect against cyber threats. We offer a comprehensive range of services tailored to meet the unique needs of each client, including:

- **Assessments and Testing:** We offer comprehensive security assessments and penetration testing services to identify weaknesses in networks, applications, and infrastructure. Our experts employ advanced methodologies to simulate real-world attacks, enabling organizations to identify and address vulnerabilities before they can be exploited by malicious actors.
- **Training and Education:** We provide cutting-edge cybersecurity training programs that cover a wide array of topics, from secure coding practices and penetration testing to incident response and risk management. Our courses are designed to enhance the capabilities of both technical and non-technical professionals, fostering a culture of security awareness throughout organizations.
- **Advisory Services:** Our team of experienced cybersecurity experts offers strategic advisory services to assist organizations in identifying vulnerabilities, developing robust security strategies, and implementing effective risk mitigation measures. We conduct comprehensive assessments, provide actionable recommendations, and support the implementation of security controls aligned with industry best practices.
- **Product and Process Evaluation:** We assist organizations in evaluating the security of their software, systems, and processes throughout the development lifecycle. Our expertise includes secure design and architecture review, threat modeling, code review, and secure SDLC assessments, ensuring that security is integrated seamlessly into every aspect of the development process.
- **Awareness and Outreach:** We recognize the critical role of security awareness in building a resilient cybersecurity culture. Through our awareness programs and outreach initiatives, we educate individuals and organizations on the latest threats, best practices, and emerging trends in cybersecurity, empowering them to make informed decisions and take proactive measures to protect themselves against cyber threats.

Security Innovation takes pride in its team of highly skilled cybersecurity professionals who possess extensive industry knowledge and expertise. We stay at the forefront of emerging threats and technologies, continuously updating our training programs and service offerings to address the evolving cybersecurity field.

With a customer-centric approach, we strive to forge long-term partnerships with our clients, providing them with the support and guidance needed to navigate the complex world of cybersecurity effectively. Whether it's a multinational corporation, government agency, or a small business, we are

dedicated to helping organizations strengthen their security posture and build resilience in the face of cyber threats.

In a world where cybersecurity is a paramount concern, Security Innovation stands as a trusted partner, offering cutting-edge solutions and expert guidance to protect the digital assets and privacy of organizations and individuals alike.

Products and Services

Our security services are at the core of what we do. It's where the company started and what fuels the content and methodologies for our Cyber Ranges, Courses, Labs, and Secure SDLC solutions. Our services focus on the software itself (whether internally built or 3rd party), the SDLC on which it's constructed, and the environment in which it's deployed. It doesn't matter if you're building something from scratch, using 3rd party components, or using commercial off the shelf software, you still must secure it in your environment, whether it's in the cloud, within your own network, or in a data center, it doesn't matter, we can help.

Services we provide:

- Application Risk Ranking
- Architecture and Design Reviews
- Attack Simulation + Red Teaming
- Cloud Configuration Reviews
- Cloud Migration Planning
- Base Camp
- CMD+CTRL / Cyber Ranges
- Learning Labs
- Training Courses
- Experts on Demand
- Penetration Testing
- SDLC Gap Analysis
- Security Code Reviews
- Smart Contract Audits
- Tabletop Exercises
- Threat Modeling
- U.S. Courts
- Kiosk Development
- Penetration Testing and Security Guidance

Description of services overview or services provided

CMD+CTRL Base Camp

CMD+CTRL Base Camp offers organizations a proven training system that provides all employees in the SDLC a base of knowledge, along with the skill sets needed, to defend against modern attacks.

Through a single portal, CMD+CTRL Base Camp offers learners progressive, blended learning experiences called Learning Journeys, which are training experiences that include a curated blend of courses, labs, and cyber ranges. Each journey is customized to specific roles or areas of expertise. Regardless of experience or skill level, every employee receives a guided path toward a learning goal you have set for them.

- **CMD+CTRL Courses:** We offer the industry's largest security library for those who build, operate, and defend software. Our micro-learning approach makes it a cinch to build target skills with turn-key but customizable Learning Paths geared toward all roles and skill levels across the SDLC.
- **CMD+CTRL Labs:** Labs reinforce computer-based training courses by guiding your team through practical, hands-on exercises. Each simulation provides learners with vivid examples of real-world threat scenarios, then helps transform those experiences into tangible skills they can apply every day.
- **CMD+CTRL Cyber Range:** The Cyber Range is a hands-on training platform that uses purposely insecure software environments to hone security skills. It reflects the complexity and risk of today's tech stacks: flawed design, defenseless code, and misconfigured deployments – and tempts players to exploit them.

CMD+CTRL support teams are available during regular business hours for any assistance you require – including setup and deployment, goal setting, learning journeys, technical assistance and more.

CMD+CTRL Base Camp is available as an annual subscription with no apps to download, and no special equipment needed. Your team receives access to our entire library of over 350 courses and labs, along with one of our 11 infamous Cyber Range experiences.

U.S. Courts

Penetration Testing and Kiosk Development.

- **Penetration testing:** The Security Innovation U.S. Courts Application Team assists the U.S. Federal Courts in ensuring the security of the PACER (Public Access to Court Electronic Records) system. The team performs penetration testing, provides security guidance, and incident response services to the PACER development team.
- **Kiosk Development:** The Security Innovation U.S. Courts Development Team develops and maintains a secure kiosk operating system for accessing the PACER system, and individual courts websites, that is deployed in federal courthouses across the nation.

DC 2: The Principal Service Commitments and System Requirements

Security Innovation designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Security Innovation makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Security Innovation has established for the services. The system services are subject to the Security and Availability commitments established internally for its services.

Security Innovation's commitments to users are communicated through Master Service Agreements (MSAs), online Privacy Policy, and Release Documentation.

Security commitments include, but are not limited to, the following:

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system.
- Regular vulnerability scans over the system and network, and penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.
- Up time availability of production systems.

Availability commitments include, but are not limited to, the following:

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a reasonably timely manner.
- Business continuity and disaster recovery plans that include detailed instructions, recovery point objectives (RPOs), recovery time objectives (RTOs), roles, and responsibilities.
- Operational procedures supporting the achievement of availability commitments to user entities.

DC 3: The Components of the System Used to Provide the Services

The System description is comprised of the following components:

- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- Data – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- Procedures – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

3.1 Primary Infrastructure

Security Innovation maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description, and owner.

Hardware	Type	Purpose
AWS Elastic Compute Cloud (EC2)	AWS	Provide scalable computing capacity
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

3.2 Primary Software

Security Innovation is responsible for managing the development and operation of the CMD+CTRL Basecamp system including infrastructure components such as servers, databases, and storage systems. The in-scope Security Innovation infrastructure and software components are shown in the table provided below:

System/Application	Operating System	Purpose
15 Five	Cloud	Performance Tracking
Alienvault	Cloud	Centralized Logging
Amazon Web Services	Cloud	PaaS
Backupify	Cloud	Google Suite Data Backup
Box	Cloud	Secure File Repository with BYOK
Brivo Badge System	Cloud	Office Location Badge System
Confluence	Cloud	Wiki – Document Management
Duo	Cloud	2 Factor Authentication Services
GitLab	Cloud	Source Code Repository
Google Workspace	Cloud	Email, Calendar
ISP Comcast	Cloud	Internet Service
ISP Lumen	Cloud	Internet Service
Jira	Cloud	Bug, Hotfix, Release Tracking
JumpCloud	Cloud	Central Authentication Directory
Lever	Cloud	Job Posting
New Relic	Cloud	SLA Monitoring
PagerDuty	Cloud	DR and Escalation
Portswigger/Burp Suite	Cloud	Vulnerability Scanning Tool
Qualys	Cloud	Vulnerability Scanning Tool
Slack	Cloud	Communication and Collaboration
Sophos	Cloud	Antivirus
Unifi Networks	Cloud	Office Networks
Vanta	Cloud	Compliance Tracking
Verkada Cameras	Cloud	Office CCTV
Zoom	Cloud	Communication Tool

3.3 People

The company employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Security Innovation has a staff of approximately 150 people organized in the following functional areas:

Group/Role Name	Function
Executive Management	Responsible for overseeing company-wide activities, establishing and accomplishing goals, and overseeing objectives.
Engineering – CMD+CTRL	Responsible for the CMD+CTRL development, testing, deployment, security, and maintenance of the CMD+CTRL Platform.
Engineering – US Courts	Responsible for the US Courts development, testing, deployment, security, and maintenance of the Courts Kiosk Platform.
eKnowledge	Responsible for maintaining our learning labs, course catalog, and training simulators.
Product	Responsible for the product life cycle, including adding new product functionality as well as user interface (UI) and user experience (UX) design features and enhancements.
Services	Responsible for conducting customer penetration testing and security services.
Sales	Responsible for the qualification and negotiation of prospective customers.
Marketing	Responsible for company marketing and promotions across all platforms.
Finance & Operations	Responsible for maintaining internal processes, tools and systems to support the finance and business operations teams.
Legal, People, and Culture	Responsible for legal, risk management, compliance, people administration, and partner relations.

3.4 Data

Data as defined by Security Innovation, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Security Innovation:

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Security Innovation.	● Press releases ● Public website
Internal	Access to internal information is approved by management and is protected from external access.	● Internal memos ● Design document ● Product specifications ● Correspondences
Customer Data	Information received from customers for processing or storage by Security Innovation. Security Innovation must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Customer operating data ● Customer PII ● Customers' customers' PII ● Anything subject to a confidentiality agreement with a customer
Company Data	Information collected and used by Security Innovation to operate the business. Security Innovation must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	● Legal documents ● Contractual agreements ● Employee PII ● Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Security Innovation has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.5 Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

3.5.1 Physical Security

Security Innovation's production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Security Innovation reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

3.5.2 Logical Access

Security Innovation provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and reportable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no-access roles. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Information Technology is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Security Innovation's policies, completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Information Technology is responsible for deprovisioning access to all in-scope systems within 2 days of that employee's termination.

3.5.3 Computer Operations - Backups

Customer data is backed up and monitored by the DevOps team which ensures the backup of all production systems and on the corporate side the IT team is responsible for disaster recovery. for completion and exceptions. If there is an exception, The DevOps team ensures the backup of all production systems and on the corporate side the IT team is responsible for disaster recovery. will perform troubleshooting to identify the root cause and either rerun the backup or as part of the next scheduled backup job.

Backup infrastructure is maintained in AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer Operations - Availability

Security Innovation maintains an incident response plan to guide employees on reporting and responding to any information security or data privacy events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Security Innovation internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Security Innovation utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

3.5.5 Change Management

Security Innovation maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

3.5.6 Data Communications

Security Innovation has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Security Innovation application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Security Innovation conducts monthly internal and external vulnerability scans of all IT, Production, and Development Environments. We also have deployed Intrusion Detection systems on both host and network levels which store data in a centralized logging service. This data is reviewed monthly during IT and Engineering meetings.

3.6 Boundaries of the System

The boundaries of the CMD+CTRL Basecamp are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the CMD+CTRL Basecamp.

DC 4: Disclosures about Identified Security Incidents

There have been no significant incidents to the system in the past six (6) months that have impacted our business.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization's Service Commitments and System Requirements were Achieved

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

5.1 Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are essential elements of Security Innovation's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Security Innovation's ethical and behavioral standards, how they are communicated, and how they are reinforced in practices. 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.

Specific control activities that the service organization has implemented in this area are described below:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

5.2 Commitment to Competence

Security Innovation's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for particular jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

5.3 Management's Philosophy and Operating Style

The Security Innovation management team must balance two competing interests: continuing to grow and develop in a cutting-edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Security Innovation can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally, any regulatory changes that may require Security Innovation to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with our core product offerings and duties to new and existing customers.

Specific control activities that the service organization has implemented in this area are described below:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

5.4 Organizational Structure and Assignment of Authority and Responsibility

Security Innovation's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Security Innovation's assignment of authority and responsibility activities include factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity’s objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

5.5 HR Policies and Practices

Security Innovation's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top-quality personnel who ensure the service organization is operating at maximum efficiency. Security Innovation's human resources policies and practices relating to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgement forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk Assessment Process

Security Innovation's risk assessment process identifies and manages risks that could potentially affect Security Innovation's ability to provide reliable and secure services to our customers. As part of this process, Security Innovation maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Security Innovation product development process so they can be dealt with predictably and iteratively.

5.7 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Security Innovation's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Security Innovation addresses these risks through the implementation of suitably designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Security Innovation's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and Communication Systems

Information and communication are an integral component of Security Innovation'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 the entity's operations.

Security Innovation uses several information and communication channels internally to share information with management, employees, contractors, and customers. Security Innovation uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, Security Innovation uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring Controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Security Innovation's management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

5.9.1 On-going Monitoring

Security Innovation's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Security Innovation's operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision for addressing any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Security Innovation's personnel.

5.10 Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

DC 6: Complementary User Entity Controls (CUECs)

Security Innovation'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 Trust Services Criteria related to Security Innovation's services to be solely achieved by Security Innovation control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Security Innovation's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services 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 their contractual obligations to Security Innovation.
- User entities are responsible for notifying Security Innovation of changes made to technical or administrative contact information.
- User entities are responsible for maintaining their own system(s) of record.
- User entities are responsible for ensuring the supervision, management, and control of the use of Security Innovation services by their personnel.
- User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Security Innovation services.
- User entities are responsible for providing Security Innovation with a list of approvers for security and system configuration changes for data transmission.
- User entities are responsible for immediately notifying Security Innovation of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

DC 7: Complementary Subservice Organization Controls (CSOCs)

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities.

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entities services.

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

The following subservice organization controls have been implemented by AWS and included in this report to provide additional assurance that the trust services criteria are met.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Availability	A 1.2	AWS maintains formal policies that provide guidance for information security within the organization and the supporting IT environment.
Availability	A 1.2	AWS has a process in place to review environmental and geo-political risks before launching a new region.
Availability	A 1.2	Amazon-owned data centers are protected by fire detection and suppression systems.

Category	Criteria	Control
Availability	A 1.2	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.
Availability	A 1.2	Uninterruptible Power Supply (UPS) units provide backup power in the event of an electrical failure in Amazon owned data centers
Availability	A 1.2	Amazon-owned data centers have generators to provide backup power in case of electrical failure.
Availability	A 1.2	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. Contracts also include provisions requiring communication of incidents or events that impact Amazon assets and/or customers to AWS.

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

- Reviewing and reconciling output reports
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

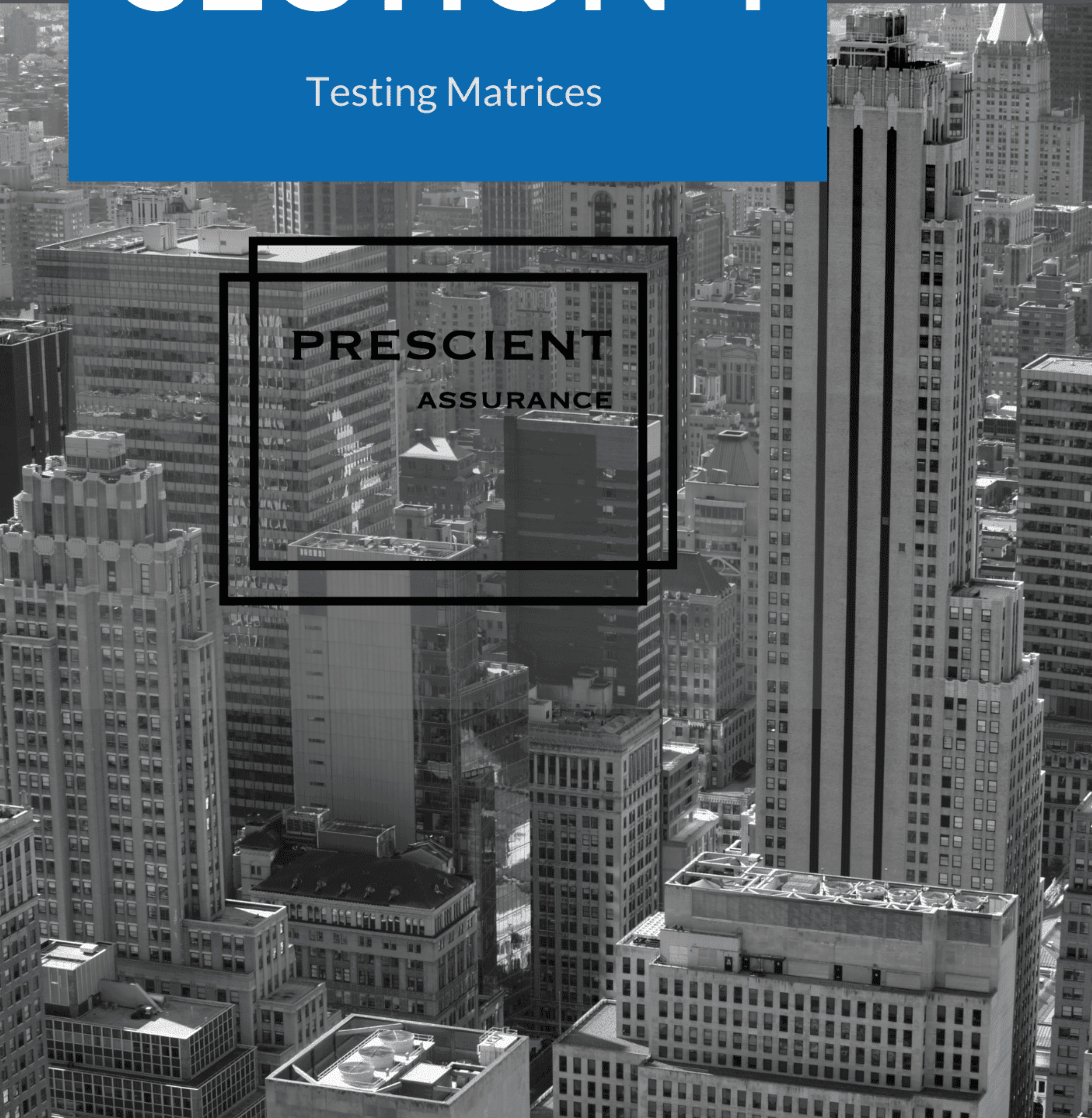
All Security, and Availability criteria were applicable to the Security Innovation's CMD+CTRL Basecamp system.

DC 9: Disclosures of Significant Changes In Last 1 Year

There have been no major changes to the system in the past three (3) months that have impacted our business.

SECTION 4

Testing Matrices



PRESCIENT

ASSURANCE

Tests of Design of Controls and Results of Tests

Scope of Testing

This report on the controls relates to CMD+CTRL provided by Security Innovation. The scope of the testing was restricted to CMD+CTRL, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing as of July 17, 2023.

The tests applied to test the Design of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that all applicable trust services criteria were achieved during the review date. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates.
- The control risk mitigated by the control.
- The effectiveness of entity-level controls, especially controls that monitor other controls.
- The degree to which the control relies on the effectiveness of other controls.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our audit procedures and tests performed to evaluate the design effectiveness of the controls detailed in the matrices that follow:

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.

Inspection	Inspected documents and records indicating the performance of the control. This includes, but is not limited to, the following: ● Examination / Inspection of source documentation and authorizations to verify transactions processed. ● Examination / Inspection of documents or records for evidence of performance, such as the existence of initials or signatures. ● Examination / Inspection of systems documentation, configurations, and settings; and ● Examination / Inspection of procedural documentation such as operations manuals, flow charts, and job descriptions.
Observation	Observed the implementation, application, or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and/or operation of the control activity as performed if applicable.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices.

Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Design Effectiveness of the control activity.

Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	The company evaluates system capacity on an ongoing basis, and system changes are implemented to help ensure that processing capacity can meet demand.	Inspected the Operations Security Policy to determine that the use of processing resources and system storage is required to be monitored and adjusted to ensure that system availability and performance meet the company's requirements.	No exceptions noted.
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.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Operations Security Policy to determine that the company is required to configure production infrastructure to produce detailed logs containing user activities, exceptions, faults, and information security events produced, kept, and reviewed through manual or automated processes as needed.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	Observed the company's AWS RDS console showing two different availability zones enabled to determine that the company has a multi-location strategy for production environments employed to permit the resumption of operations at other company data centers in the event of loss of a facility.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery	The company's databases are replicated to a secondary data center in real-time. Alerts are configured to notify administrators if replication fails.	Observed that all Amazon RDS instances have backups enabled to determine that databases are replicated to a secondary data center in real-time.	No exceptions noted.

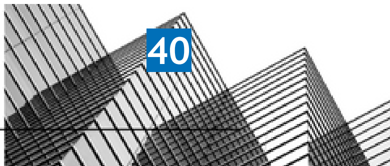
	infrastructure to meet its objectives.			
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company performs regularly for production data. Data is backed up to a different location than the production system.	Inspected the Operations Security Policy to determine that the company is required to take backup copies regularly and test its backup processes at least annually.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company'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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to conduct annual disaster recovery tests.	No exceptions noted.
A1.2	The entity authorizes, designs, develops or acquires, implements,	The company has a documented risk management program	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to	No exceptions noted.

	operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	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 for those risks.	be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	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.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the roles and responsibilities have been established to execute the communication plan and strategy for the continuity of critical services.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operations Security Policy to determine that production systems are required to be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to conduct annual disaster recovery tests.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company is required to perform background verification checks on all employees.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company is required to evaluate each employee's performance annually, based on an assessment of job performance, competence in the role, adherence to company policies and code of conduct,	No exceptions noted.

			and achievement of role-specific objectives.	
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the Human Resource Security Policy to determine that all employees are required to sign a confidentiality agreement upon hire.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the Human Resource Security Policy to determine that contractors are required to sign a confidentiality agreement upon hire.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	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.	Inspected the Code of Conduct to determine that the company requires all employees to acknowledge the Code of Conduct at the time of hire. Inspected the Human Resource Security Policy to determine that the company has defined a progressive disciplinary process to be implemented against employees who violate the Code of Conduct.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Code of Conduct to determine that the company requires all contractor staff to abide by the Code of Conduct.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	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.	Inspected the meeting minutes of a board meeting to determine that the company's board meetings are conducted at least annually.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information	Inspected the LinkedIn profiles showing the skills, education, and experiences of board members and executive leadership to determine that the board members are qualified enough to manage the company's information security controls.	No exceptions noted.

		security experts and consultants as needed.		
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the meeting minutes of a board meeting to determine that the company's board meetings are conducted at least annually. Inspected the LinkedIn profile of board members to determine that the board includes directors that are independent of the company.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Information Security Roles and Responsibilities to determine that the responsibilities of the board of directors for oversight of internal controls have been defined.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Information Security Roles and Responsibilities to determine that the responsibilities of the board of directors for oversight of internal controls have been defined.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Observed the company's organizational chart showing that the company is headed by the CEO to determine that the company maintains an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner among others, for the design and implementation of information security controls.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner and employees have been defined for the management of information security controls.	No exceptions noted.

		the Roles and Responsibilities policy.		
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the Human Resource Security Policy to determine that the company requires all employees to complete security awareness training upon hire and annually after that.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected the Human Resource Security Policy to determine that the company is required to perform background verification checks on all employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company is required to evaluate each employee's performance annually, based on an assessment of job performance, competence in the role, adherence to company policies and code of conduct, and achievement of role-specific objectives.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	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.	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner and employees have been defined for the management of information security controls.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	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.	Inspected the Code of Conduct to determine that the company requires all employees to acknowledge the Code of Conduct at the time of hire. Inspected the Human Resource Security Policy to determine that the company has defined a progressive disciplinary process to be implemented against employees who violate the Code of Conduct.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected the Human Resource Security Policy to determine that the company is required to evaluate each employee's performance annually, based on an assessment of job performance, competence in the role, adherence to company policies and code of conduct,	No exceptions noted.



			and achievement of role-specific objectives.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	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.	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner and employees have been defined for the management of information security controls.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Observed that the company uses Vanta for continuous security monitoring.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least monthly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the production environment at least monthly.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	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.	Inspected the Operations Security Policy to determine that the company is required to log and monitor all events related to user activities, exceptions, faults, and information security to achieve its security and monitoring objectives.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected the Human Resource Security Policy to determine that the company requires all employees to complete security awareness training upon hire and annually after that.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal	The company communicates system changes to authorized internal users.	Inspected the Operations Security Policy to determine that the company requires all system changes to be communicated	No exceptions noted.

	control, necessary to support the functioning of internal control.		to relevant internal stakeholders in advance.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	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.	Inspected the Information Security Policy to determine that the company requires all users to report known or suspected security events or incidents, including policy violations and observed security weaknesses, as soon as possible by sending an email to the relevant address mentioned.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company's website to determine that descriptions of the company's products and services have been provided to internal and external users through the main page.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner among others, for the design and implementation of information security controls.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually and acknowledged by employees and contractors.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner and employees have been defined for the	No exceptions noted.

		assigned in job descriptions and/or the Roles and Responsibilities policy.	management of information security controls.	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the company's Security Page to determine that security commitments are communicated to users through the website.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company's website to determine that descriptions of the company's products and services have been provided to internal and external users through the main page.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected the Operations Security Policy to determine that the company requires all system changes to be communicated to the relevant external stakeholders in advance.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the support page on the company's website to determine that external support resources relating to system operations are available.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	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.	Inspected the company's website which provides a contact us and support page to determine that the company has an external-facing support system in place.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality and privacy commitments.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy to determine that the company has developed its risk management procedures to address its strategic and operational objectives.	No exceptions noted.

CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	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 for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The 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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to conduct annual disaster recovery tests.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The 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.	Inspected the Third Party Management Policy to determine that the company has a vendor management program in place which addresses third-party monitoring, security standards, risk management, and annual evaluations of service delivery and supplier security.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity	The company has a documented risk management program	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to	No exceptions noted.

	and analyzes risks as a basis for determining how the risks should be managed.	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 for those risks.	be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.

		strategies for those risks.		
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine that the company requires systems and networks to be provisioned and maintained in accordance with the company's configuration and hardening standards.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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.	Inspected the Operations Security Policy to determine that the company is required to perform penetration tests of the applications and production network annually.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least monthly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the production environment at least monthly.	No exceptions noted.

CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	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.	Inspected the Operations Security Policy to determine that the company is required to perform penetration tests of the applications and production network annually.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	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.	Inspected the Third Party Management Policy to determine that the company has a vendor management program in place which addresses third-party monitoring, security standards, risk management, and annual evaluations of service delivery and supplier security.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually. Observed that the company uses Vanta for continuous security monitoring.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	The company 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.	Inspected the Third Party Management Policy to determine that the company has a vendor management program in place which addresses third-party monitoring, security standards, risk management, and annual evaluations of service delivery and supplier security.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those	The company performs control self-assessments at least annually to gain	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.

	parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Observed that the company uses Vanta for continuous security monitoring.	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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 for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually and acknowledged by employees and contractors.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC5.2	The entity also selects and develops general control	The company's information security	Inspected the Human Resources Security Policy to determine that the	No exceptions noted.

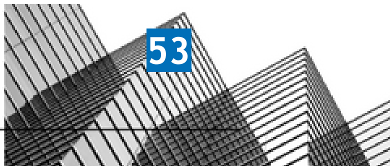
	activities over technology to support the achievement of objectives.	policies and procedures are documented and reviewed at least annually.	management is required to ensure that the policies and procedures have been reviewed annually and acknowledged by employees and contractors.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal data retention and disposal procedures have been established stating that Security Innovation is required to retain data as long as the company has a need for its use. Additionally, the policy defines the retention periods of various data types.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that information backup requirements have been documented stating that backup copies are required to be taken regularly and restore capabilities are required to be tested periodically, not less than annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the Human Resources Security Policy to determine that the management is required to ensure that the policies and procedures have been reviewed annually and acknowledged by employees and contractors.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures	The company specifies its objectives to enable the identification and assessment of risk	Inspected the Risk Management Policy to determine that the company has developed its risk management procedures to address its strategic and operational objectives.	No exceptions noted.

	that put policies into action.	related to the objectives.		
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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 for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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.	Inspected the Third Party Management Policy to determine that the company has a vendor management program in place which addresses third-party monitoring, security standards, risk management, and annual evaluations of service delivery and supplier security.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or	Inspected the Information Security Roles and Responsibilities Policy to determine that specific responsibilities have been assigned to the Board of Directors, Executive Leadership, Director of IT, VP of Engineering, Director of Customer Support, and system owner and employees have been defined for the management of information security controls.	No exceptions noted.

		the Roles and Responsibilities policy.		
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the Access Control Policy to determine that the company has documented requirements for complex passwords of confidential systems.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Cryptography Policy to determine that access to keys and secrets is required to be tightly controlled in accordance with the Access Control Policy.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH keys.	Inspected the Access Control Policy to determine that the company requires all personnel to have a unique user identifier for system access and use MFA for privileged access to the production infrastructure.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to databases to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege and restricts access to authorized employees with business needs.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the application to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege and restricts access to authorized employees with business needs.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that the company is required to use multi-factor authentication (MFA) to enforce unique production infrastructure authentication.	No exceptions noted.

CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege and restricts access to authorized employees with business needs.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company 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.	Inspected the Access Control Policy to determine that the company requires all access and rights modification requests to be documented in an access request ticket, or email, and approval is required from the system or data owner, or management.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the Access Control Policy to determine that the company is required to encrypt all remote connections to the production systems and networks.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have unique user identifiers and strong passwords for system access.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the Secure Development Policy to determine that all Security Innovation software is version controlled and synced between developers and access to the central repository is restricted based on an employee's role.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of least privilege and restricts access to authorized employees with business needs.	No exceptions noted.
CC6.1	The entity implements logical access security	The company has a data classification	Inspected the Data Management Policy to determine that the company has	No exceptions noted.

	software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	established a data classification scheme and handling procedures for confidential, public, and restricted data.	
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected the Cryptography Policy to determine that the company is required to use AES-256-bit encryption for confidential data at rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the Information Security and Acceptable Use Policy to determine that the use of remote access software and/or services are allowable as long as it is provided by the company and configured for MFA.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the Operations Security Policy to determine that the development and staging environments are required to be strictly segregated from production environments to reduce the risks of unauthorized access or changes to the operational environment.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company maintains a formal inventory of production system assets.	Inspected the Asset Management Policy to determine that the company is required to maintain an inventory of assets associated with information and information processing facilities that store, process, or transmit classified information.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	The company restricts privileged access to the operating system	Inspected the Access Control Policy to determine that the company grants users access to company systems and applications based on the principle of	No exceptions noted.



	protected information assets to protect them from security events to meet the entity's objectives.	to authorized users with a business need.	least privilege and restricts access to authorized employees with business needs.	
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.	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.	Inspected the Access Control Policy to determine that the company requires all access and rights modification requests to be documented in an access request ticket, or email, and approval is required from the system or data owner, or management.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have unique user identifiers and strong passwords for system access.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke access for terminated employees within 24 business hours of termination of contract or employment.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed	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.	Inspected the Access Control Policy to determine that administrators are required to perform access rights reviews of user, administrator, and service accounts on a quarterly basis.	No exceptions noted.

	when user access is no longer authorized.			
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.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the Access Control Policy to determine that the company has established access control procedures, including access provisioning, de-provisioning, access change, and review procedures.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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.	Inspected the Access Control Policy to determine that administrators are required to perform access rights reviews of user, administrator, and service accounts on a quarterly basis.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	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.	Inspected the Access Control Policy to determine that the company requires all access and rights modification requests to be documented in an access request ticket, or email, and approval is required from the system or data owner, or management.	No exceptions noted.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have unique user identifiers and strong passwords for system access.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke access for terminated employees within 24 business hours of termination of contract or employment.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	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.	Inspected the Access Control Policy to determine that administrators are required to perform access rights reviews of user, administrator, and service accounts on a quarterly basis.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company has processes in place for granting, changing, and terminating physical access to company data centers based on an authorization from control owners.	Inspected the Physical Security Policy to determine that the company requires secure areas to be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	No exceptions noted.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to	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.	Inspected the Physical Security Policy to determine that third-parties in secure areas are required to sign in and out on a visitor log and should be escorted or monitored by Security Innovation personnel.	No exceptions noted.

	meet the entity's objectives.			
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The company reviews access to the data centers at least annually.	Inspected the Physical Security Policy to determine that the company requires secure areas to be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected the Access Control Policy to determine that the company is required to revoke access for terminated employees within 24 business hours of termination of contract or employment.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the Data Management Policy to determine that the company has the option to use an E-Waste service for data destruction and is required to retain the certificates of destruction on record for one year.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Management Policy to determine that the company has defined secure data disposal procedures to be followed for deleting confidential data when no longer needed.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the Data Management Policy to determine that internal data retention and disposal procedures have been established stating that Security Innovation is required to retain data as long as the company has a need for its use. Additionally, the policy defines the retention periods of various data types.	No exceptions noted.

CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Data Management Policy to determine that the company is required to encrypt all confidential data during transit.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operations Security Policy to determine that production systems are required to be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the Operations Security Policy to determine that the company requires production network access configuration rules to be reviewed at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the Operations Security Policy to determine that the company is required to use firewalls to control network traffic to and from the production environment.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	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.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that the IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that the company has defined standards for network and system hardening and that production network access configuration rules shall be reviewed at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor	Inspected the Information Security and Acceptable Use Policy to determine that the use of remote access software and/or services are allowable as long as it is provided by the company and configured for MFA.	No exceptions noted.

		authentication (MFA) method.		
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected the Access Control Policy to determine that all personnel are required to have unique user identifiers and strong passwords for system access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the Access Control Policy to determine that the company is required to encrypt all remote connections to the production systems and networks.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the Information Security Policy to determine that all end-user devices must comply with the policy and that any mobile device used to access company resources is not to be shared with others. Observed that the company uses Vanta as an MDM.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the Data Management Policy to determine that the company is required to encrypt all confidential data during transit.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Inspected the Data Management Policy to determine that the company requires mobile device hard drives containing confidential data to be encrypted and prohibits confidential data from being stored on removable media.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks	Inspected the Operations Security Policy to determine that the company is required to install anti-malware protections on all company-issued endpoints.	No exceptions noted.

	software to meet the entity's objectives.	and configures this to be updated routinely, logged, and installed on all relevant systems.		
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company 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.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that the IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
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.	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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to	Host-based vulnerability scans are performed at least monthly on all	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the	No exceptions noted.

	configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	external-facing systems. Critical and high vulnerabilities are tracked to remediation.	production environment at least monthly.	
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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
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.	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.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes.	No exceptions noted.
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.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the Operations Security Policy to determine that the company requires systems and networks to be provisioned and maintained in accordance with the company's configuration and hardening standards.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the Operations Security Policy to determine that the company is required to configure production infrastructure to produce detailed logs containing user activities, exceptions, faults, and information security events produced, kept, and reviewed through manual or automated processes as needed.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that IT and Engineering departments are	No exceptions noted.

	affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	management; - system monitoring.	responsible to evaluate the severity of vulnerabilities.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the Operations Security Policy to determine that the company is required to log and monitor all events related to user activities, exceptions, faults, and information security to achieve its security and monitoring objectives.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company 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.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that the IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the Operations Security Policy to determine that the company is required to perform penetration tests of the applications and production network annually.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the Operations Security Policy to determine that production systems are required to be configured to monitor, log, and self-repair and/or alert on suspicious changes to critical system files where feasible.	No exceptions noted.

CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Host-based vulnerability scans are performed at least monthly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the production environment at least monthly.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The 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.	Inspected the Incident Response Plan to determine that the incident response phases including the roles and responsibilities of the Incident Response Team to manage security or data privacy events have been documented.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company tests their incident response plan at least annually.	Inspected the company's Incident Response Plan to determine that the company ensures that the Incident Response plans meets industry standards and is updated annually. Inspected the Incident Response Plan Tabletop exercise completed on June 28, 2023 to determine that the company tests their incident response plan at least annually.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The 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	Inspected the Incident Response Plan to determine that the incident response phases including the roles and responsibilities of the Incident Response Team to manage security or data privacy events have been documented.	No exceptions noted.

		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.	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.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that the IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least monthly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the production environment at least monthly.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company is required to conduct annual disaster recovery tests.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	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.	Inspected the Incident Response Plan to determine that the incident response phases including the roles and responsibilities of the Incident Response Team to manage security or data privacy events have been documented.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the company's Incident Response Plan to determine that the company ensures that the Incident Response plans meets industry standards and is updated annually.	No exceptions noted.

			Inspected the Incident Response Plan Tabletop exercise completed on June 28, 2023 to determine that 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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan to determine that the company has documented the procedures to assess and respond to an information security incident.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company 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.	Inspected the Operations Security Policy to determine that a change management process has been documented stating the stages of planning, testing, approving, communicating, and documenting changes.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the Secure Development Policy to determine that the company has described secure system engineering principles, change control procedures, and version control guidelines.	No exceptions noted.
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.	Host-based vulnerability scans are performed at least monthly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected the Operations Security Policy to determine that vulnerability scans are required to be run on the production environment at least monthly.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to	The company's penetration testing is performed at least annually. A remediation plan is	Inspected the Operations Security Policy to determine that the company is required to perform penetration tests of the applications and production network annually.	No exceptions noted.

	infrastructure, data, software, and procedures to meet its objectives.	developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.		
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that the company has defined standards for network and system hardening and that production network access configuration rules shall be reviewed at least annually.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the Secure Development Policy to determine that all Security Innovation software is version controlled and synced between developers and access to the central repository is restricted based on an employee's role.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	The company has 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.	Inspected the Operations Security Policy to determine that vulnerability management and system monitoring procedures have been documented by the company stating that the IT and Engineering departments are responsible to evaluate the severity of vulnerabilities.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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.	Inspected the Risk Management Policy to determine that the company is required to perform a formal risk assessment at least annually.	No exceptions noted.

CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the roles and responsibilities have been established to execute the communication plan and strategy for the continuity of critical services.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the Risk Management Policy which states that the company may use insurance as protection against financial loss to determine that the company is entitled to maintain cybersecurity insurance if necessary.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 for those risks.	Inspected the Risk Management Policy to determine that the company requires a risk register to be maintained, risks to be ranked and assessed, their impact analyzed, and relevant responses implemented as part of its risk management program.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	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.	Inspected the Third Party Management Policy to determine that the company has a vendor management program in place which addresses third-party monitoring, security standards, risk management, and annual evaluations of service delivery and supplier security.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the Third Party Management Policy to determine that the company requires agreements to be signed with vendors to acknowledge their confidentiality and privacy commitments.	No exceptions noted.