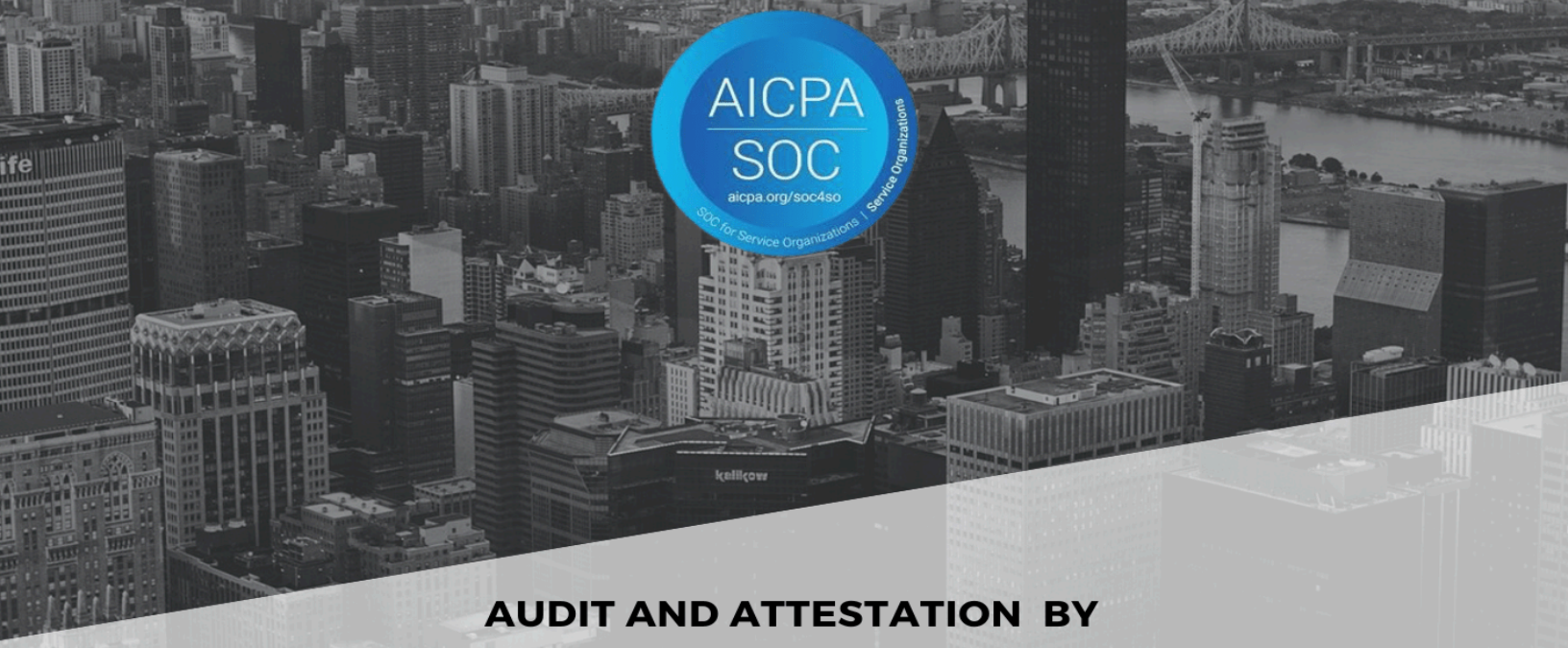
SOC 2 Type 1 Report

Bryllyant, Inc.

January 10, 2024

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



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 Bryllyant, Inc.'s system as of December 18, 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 Bryllyant, Inc.'s system that may be useful when assessing the risks arising from interactions with Bryllyant, Inc.'s system, particularly information about system controls that Bryllyant, Inc. 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 set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

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

A. The description presents Bryllyant, Inc.'s system that was designed as of December 18, 2023, in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of December 18, 2023, to provide reasonable assurance that Bryllyant, Inc.'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 Bryllyant, Inc.'s controls as of that date.

DocuSigned by:
Brandon Geise
0AA93425119444B...

Brandon Geise

CEO of Bryllyant, Inc.

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Bryllyant, Inc.

Scope

We have examined Bryllyant, Inc.'s ("Bryllyant, Inc.") accompanying description of its system as of December 18, 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 December 18, 2023, to provide reasonable assurance that Bryllyant, Inc.'s service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.*

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

Bryllyant, Inc. 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 Bryllyant, Inc.'s service commitments and system requirements were achieved. In Section 1, Bryllyant, Inc. has provided the accompanying assertion titled "Management's Assertion of Bryllyant, Inc." (assertion) about the description and the suitability of design of controls stated therein. Bryllyant, Inc. is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditors' Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design 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 Bryllyant, Inc.'s system that was designed as of December 18, 2023 in accordance with the description criteria.
B. The controls stated in the description were suitably designed as of December 18, 2023, to provide reasonable assurance that Bryllyant, Inc.'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 Bryllyant, Inc.'s controls as of that date.

Restricted Use

This report is intended solely for the information and use of Bryllyant, Inc., user entities of Bryllyant, Inc.'s system as of December 18, 2023, business partners of Bryllyant, Inc. 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
January 10, 2024

SECTION 3

System Description

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

COMPANY BACKGROUND

Bryllyant (the "company") is a software development firm that was founded in 2016 and based out of Philadelphia, PA.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

Bryllyant provides custom software solutions that advance Bryllyant and our clients' business goals. Our services include:

- Web & Mobile App Development
- Platform and Marketplace Development
- AI & Machine Learning
- Data & Cloud
- Bryllyant custom developed services

DC 2: The Principal Service Commitments and System Requirements

Bryllyant designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Bryllyant makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Bryllyant has established for the services. The system services are subject to the Security, Confidentiality, Availability, Processing Integrity, and/or Privacy commitments established internally for its services. Commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements.

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; and
- Uptime availability of production systems.

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

- The use of encryption technologies to protect system data both at rest and in transit;
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,

- Confidential information must be used only for the purposes explicitly stated in agreements between Bryllyant and user entities.

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; and,
- 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:

- *Infrastructure* – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization uses to provide the services.
- *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

Bryllyant 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. To outline the topology of its network, the organization maintains the following network diagram.

Primary Infrastructure		
Hardware	Type	Purpose
AWS CloudFront	AWS	Content Delivery Network
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

Bryllyant is responsible for managing the development and operation of the platform including infrastructure components such as servers, databases, and storage systems. The in-scope Bryllyant infrastructure and software components are shown in the table below:

Primary Software		
System/Application	Operating System	Purpose
CloudWatch	AWS	Monitoring application used to provide monitoring, alter, and notification services for Bryllyant platform
Gitlab	Codebase	Primary repository for code

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.

Bryllyant has a staff of approximately 17 employees and contractors organized in the following functional areas:

Management - Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment.
CEO - Brandon Geiss

Operations - Responsible for maintaining the availability of production infrastructure, and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Product Development team.

Information Technology - Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development - Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

Sales and Marketing - Responsible for promoting Bryllyant's services and acquiring new customers.

3.4 Data

Data as defined by Bryllyant, constitutes the following:

- Data stored in company drives or in company-managed systems
- Data generated and/or stored by software applications developed by Bryllyant
  Data is categorized in three major types of data used by Bryllyant

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Bryllyant.	• Press releases • Public website • Marketing Materials • Release notes
Restricted	Bryllyant Inc. proprietary information requiring thorough protection; access is restricted to employees with a "need-to-know" based on business requirements. This data can only be distributed outside the company with approval	• Internal policies • Legal documents • Contracts • Employee PII • Employee salaries • Internal reports • Slack messages • Email
Confidential	Highly sensitive data requiring the highest levels of protection as described in the Data Management Policy	• Customer Data • Company financial and banking data • Incident reports • Risk assessment reports • Technical vulnerability reports • Secrets and private keys • Source code

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.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Bryllyant has policies and procedures in place to ensure 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. Reviews of these procedures are performed annually and changes are authorized by management. 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

PHYSICAL SECURITY

Bryllyant's production servers are maintained by Amazon Web Services (AWS). The physical and environmental security protections are the responsibility of AWS. Bryllyant reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

LOGICAL ACCESS

Bryllyant provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems are split into three levels: Administrator, User, and No Access. User access and roles are reviewed on a quarterly or an annual basis to ensure least privilege access.

Management is responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Bryllyant's policies and completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Management is responsible for deprovisioning access to all in-scope systems within 3 days of that employee's termination.

COMPUTER OPERATIONS - BACKUPS

Customer data is backed up and monitored by the engineering team for completion and exceptions. If there is an exception the engineering team performs troubleshooting to identify the root cause; the backup will either be rerun by the engineering team or it will run 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.

COMPUTER OPERATIONS - AVAILABILITY

Bryllyant 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.

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

Bryllyant 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.

CHANGE MANAGEMENT

Bryllyant 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.

DATA COMMUNICATIONS

Bryllyant 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 Bryllyant 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.

Bryllyant engages an external security firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The scope of this report includes the bryllyant.com website, as well as all steps of the software development life cycle for developing Bryllyant's and Bryllyant customer's systems conducted within the Bryllyant development systems.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities or any runtime application environment within the Bryllyant customers' systems.

DC 4: Disclosures About Identified Security Incidents

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the last 3 months preceding the end of the review date.

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

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

CONTROL ENVIRONMENT

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 Bryllyant's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Bryllyant'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

Bryllyant'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 Bryllyant 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 Bryllyant 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 Bryllyant 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

Bryllyant'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.

Bryllyant'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 Human Resource Policies and Practices

Bryllyant'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 ensures the service organization is operating at maximum efficiency. Bryllyant's human resources policies and practices relate 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

Bryllyant's risk assessment process identifies and manages risks that could potentially affect Bryllyant's ability to provide reliable and secure services to our customers. As part of this process, Bryllyant 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 Bryllyant 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 Bryllyant's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Bryllyant 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, Bryllyant'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 Bryllyant'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.

Bryllyant uses several information and communication channels internally to share information with management, employees, contractors, and customers. Bryllyant 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, Bryllyant 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. Bryllyant'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 are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

5.9.1 On-going Monitoring

Bryllyant'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 Bryllyant'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 Bryllyant's personnel.

REPORTING DEFICIENCIES

Bryllyant's internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding to 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)

Bryllyant'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 Bryllyant's services to be solely achieved by Bryllyant control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Bryllyant'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 Bryllyant.
- User entities are responsible for notifying Bryllyant 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 Bryllyant 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 Bryllyant services.
- User entities are responsible for providing Bryllyant with a list of approvers for security and system configuration changes for data transmission.
- User entities are responsible for immediately notifying Bryllyant 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)

SUBSERVICE ORGANIZATIONS

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

Subservice Description of Services

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

Complementary Subservice Organization Controls

Bryllyant'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 Bryllyant's services to be solely achieved by Bryllyant control procedures. Accordingly, subservice organizations, in conjunction with the

services, should establish their own internal controls or procedures to complement those of Bryllyant.

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

Category	Criteria	Control
Security	CC6.4	Physical access to data centers is approved by an authorized individual.
Security	CC6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC6.4	Closed circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC6.4	Access to server locations is managed by electronic access control devices.

Bryllyant 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, Bryllyant performs monitoring of the subservice organization controls, including the following procedures

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- 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

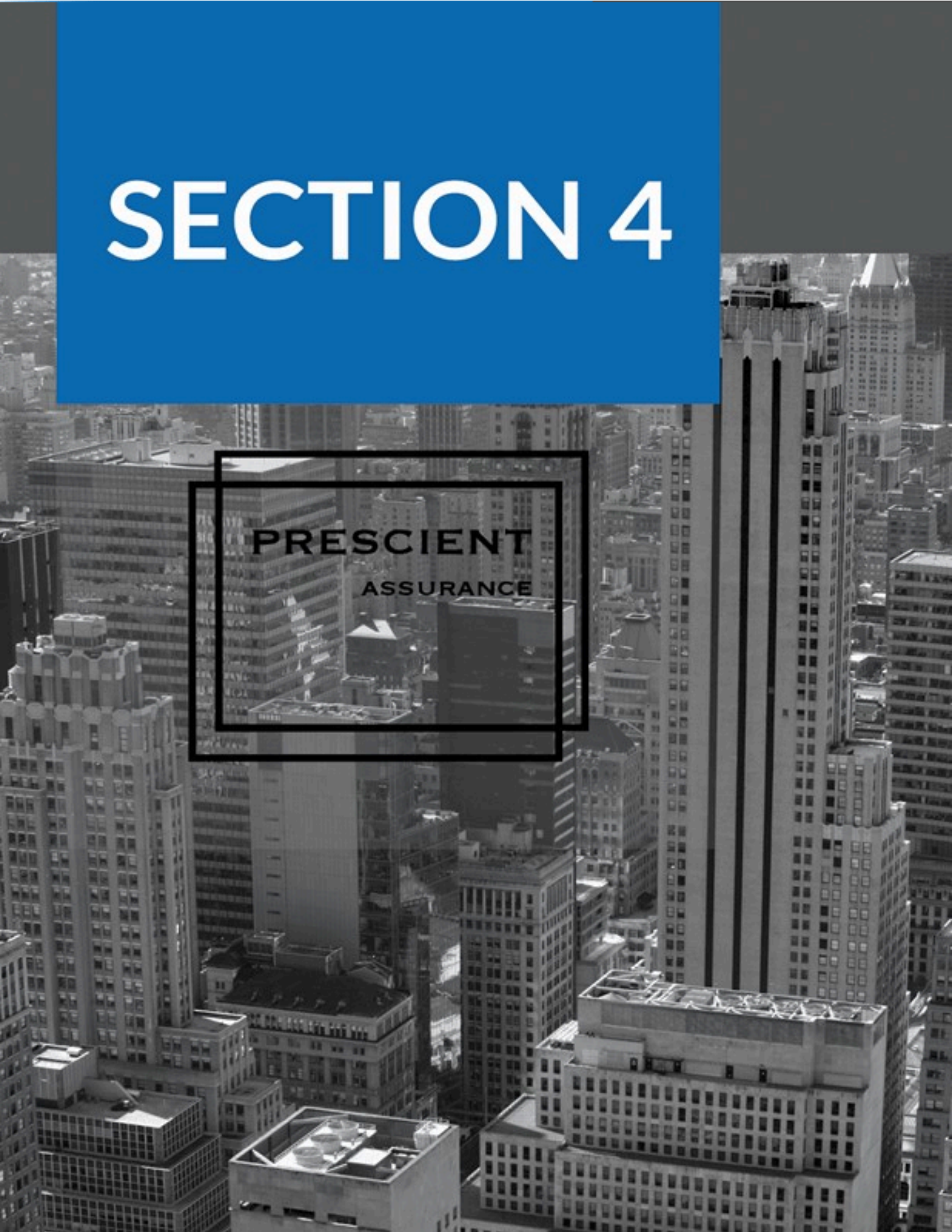
All Common Criteria/Security, Availability, Processing Integrity, Confidentiality, and Privacy criteria were applicable to the Bryllyant system.

DC 9: Disclosures Of Significant Changes In Last 1 Year

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the last 12 months preceding the end of the review date.

SECTION 4



Applicable Trust Services Criteria and Related Control Activities

Trust ID	COSO Principle	Control Description
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs background checks on new employees.
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.
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.
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.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.
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.
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.
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 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 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.
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.
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.
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.
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.
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 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 managers are required to complete performance evaluations for direct reports at least annually.

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.
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.
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.
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.
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.
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.
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.
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 quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.
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.
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.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized internal users.
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 assigned in job descriptions and/or the Roles and Responsibilities policy.
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.

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.
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.
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.
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.
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.
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.
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.
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.
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).
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.
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.
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 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.
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.
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.

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.
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.
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.
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.
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.
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.
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 strategies for those risks.
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.
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.
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.
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 quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action,	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory;

	including senior management and the board of directors, as appropriate.	- vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.
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 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.
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.
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.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.
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.
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.
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.
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.
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.
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.
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.
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 the Roles and Responsibilities policy.
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.
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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk 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 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.
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 key.
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.
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.
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 operating system to authorized users with a business need.
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.
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.
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.
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.
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.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over	The company requires passwords for in-scope system components to be configured according to the company's policy.

	protected information assets to protect them from security events to meet the entity's objectives.	
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.
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.
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 has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
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.
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.
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.
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.
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.
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.
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 conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.2	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.

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.
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.
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.
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.
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.
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.
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.
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.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is

	facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	restricted appropriately. Required changes are tracked to completion.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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.
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 authentication (MFA) method.

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.
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.
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.
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.
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 deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.
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.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.
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.
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.
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	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

	objectives; anomalies are analyzed to determine whether they represent security events.	
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.
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.
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.
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 formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	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.
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.
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.
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.
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.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.

	understand, contain, remediate, and communicate security incidents, as appropriate.	
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.
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.
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 incident response policy and procedures.
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.
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.
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.
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.
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.
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.
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 quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.
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.
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 penetration testing is performed at least annually. A remediation plan is 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 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.

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.
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.
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.
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.
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.
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.
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.