

August 29, 2024

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

In connection with your engagement to report on Tallyfy, Inc.'s (service organization) description of its Tallyfy system titled Tallyfy System Description throughout the period May 21, 2024 to August 21, 2024 (description) based on the criteria set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (description criteria) and the suitability of the design and operating effectiveness of the controls included in the description throughout the period May 21, 2024 to August 21, 2024 to provide reasonable assurance that the service organization'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* (applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented throughout the observation period in accordance with the description criteria and whether the controls stated in the description were suitably designed and operating effectively throughout the period May 21, 2024 to August 21, 2024 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.


We confirm, to the best of our knowledge and belief, as of August 29, 2024, the date of your report, the following representations made to you during your examination:

- 1) We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- 2) We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.
- 3) We have evaluated the presentation of the description in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.
- 4) We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.
- 5) We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls included in the description.
- 6) We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.
- 7) We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.

- 8) We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.
- 9) We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.
- 10) We are responsible for designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.
- 11) We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.
- 12) We have provided you with the following:
 - a) All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.
 - b) Access to additional information you have requested from us for the purpose of the engagement.
 - c) Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.
- 13) We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
- 14) We have disclosed to you any known events subsequent to the period covered by the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design or operating effectiveness of the controls, or our assertion.
- 15) We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.
- 16) We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization's system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.
- 17) We also have disclosed to you all instances about which we are aware of the following:
 - a) Misstatements and omissions in the description.
 - b) Instances in which controls have not been suitably designed or implemented as described.
 - c) Instances in which controls did not operate effectively or as described.
- 18) We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements throughout the period May 21, 2024 to August 21, 2024.
- 19) We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.
- 20) We have disclosed to you the effects of the COVID-19 pandemic on Tallyfy, Inc., its operations, and technologies used in providing services.
- 21) We have disclosed to you any communications to customers and business partners about changes in our service level agreements or commitments as a result of the COVID-19 pandemic.
- 22) We have responded fully to all inquiries made to us by you during the examination.

23) We understand that your report is intended solely for the use and information of management of the service organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information, if any. We intend to distribute your report only to those specified parties.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

DocuSigned by:

E5D5943E544C4A9
Name

CEO
Title



SOC 2 Type 2 Report

Tallyfy, Inc.

May 21, 2024 to August 21, 2024

Next Audit Window: August 22, 2024 to August 21, 2025

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security



AUDIT AND ATTESTATION BY



AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

Table of Contents

Management's Assertion	5
Independent Service Auditor's Report	8
Scope	8
Service Organization's Responsibilities	8
Service Auditors' Responsibilities	9
Inherent Limitations	9
Opinion	10
Restricted Use	10
System Description	12
DC 1: Company Overview and Types of Products and Services Provided	13
Company Background	13
Overview of the System (or Service or Product)	13
Key Features of Tallyfy	13
DC 2: The Principal Service Commitments and System Requirements	14
DC 3: The Components of the System Used to Provide the Services	14
3.1 Primary Infrastructure	15
3.2 Primary Software	17
3.3 People	18
3.4 Data	18
3.5 Processes and Procedures	20
3.6 Third Party Access	20
DC 4: Disclosures About Identified Security Incidents	20
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	21
Control Environment	21
5.1 Integrity and Ethical Values	21
5.2 Management Oversight	21
5.3 Organizational Structure	22
5.4 Assignment of Authority and Responsibility	22
5.5 Commitment to Competence	22
5.6 Accountability	22
5.7 Security Management	23
Logical Access	23
Change Management	24
Data Backup and Disaster Recovery	25
Incident Response	25
Vendor Management	26
System Monitoring	26
5.8 Information and Communications	26
5.9 Monitoring	27
5.10 Risk Assessment	27

DC 6: Complementary User Entity Controls (CUECs)	28
DC 7: Complementary Subservice Organization Controls (CSOCs)	28
DC 8: Any Specific Criterion of the Applicable Trust Services Criteria	29
DC 9: Disclosures of Significant Changes in Last 1 Year	29
Testing Matrices	29
Tests of Operating Effectiveness and Results of Tests	30
Scope of Testing	30
Types of Tests Generally Performed	30
General Sampling Methodology	31
Reliability of Information Provided by the Service Organization	32
Test Results	32



SECTION 1

Management's Assertion



Management's Assertion

We have prepared the accompanying description of Tallyfy, Inc.'s system throughout the period May 21, 2024 to August 21, 2024, 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 Tallyfy, Inc.'s system that may be useful when assessing the risks arising from interactions with Tallyfy, Inc.'s system, particularly information about system controls that Tallyfy, Inc. has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

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

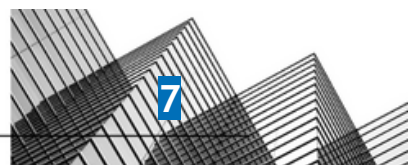
We confirm, to the best of our knowledge and belief, that:

- a. The description presents Tallyfy, Inc.'s system that was designed and implemented throughout the period May 21, 2024 to August 21, 2024 in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period May 21, 2024 to August 21, 2024, to provide reasonable assurance that Tallyfy, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Tallyfy, Inc.'s controls during that period.
- c. The controls stated in the description operated effectively throughout the period May 21, 2024, to August 21, 2024, to provide reasonable assurance that Tallyfy, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Tallyfy, Inc.'s controls operated effectively throughout the period.

DocuSigned by:

-----E5D5943F544C4A9-----

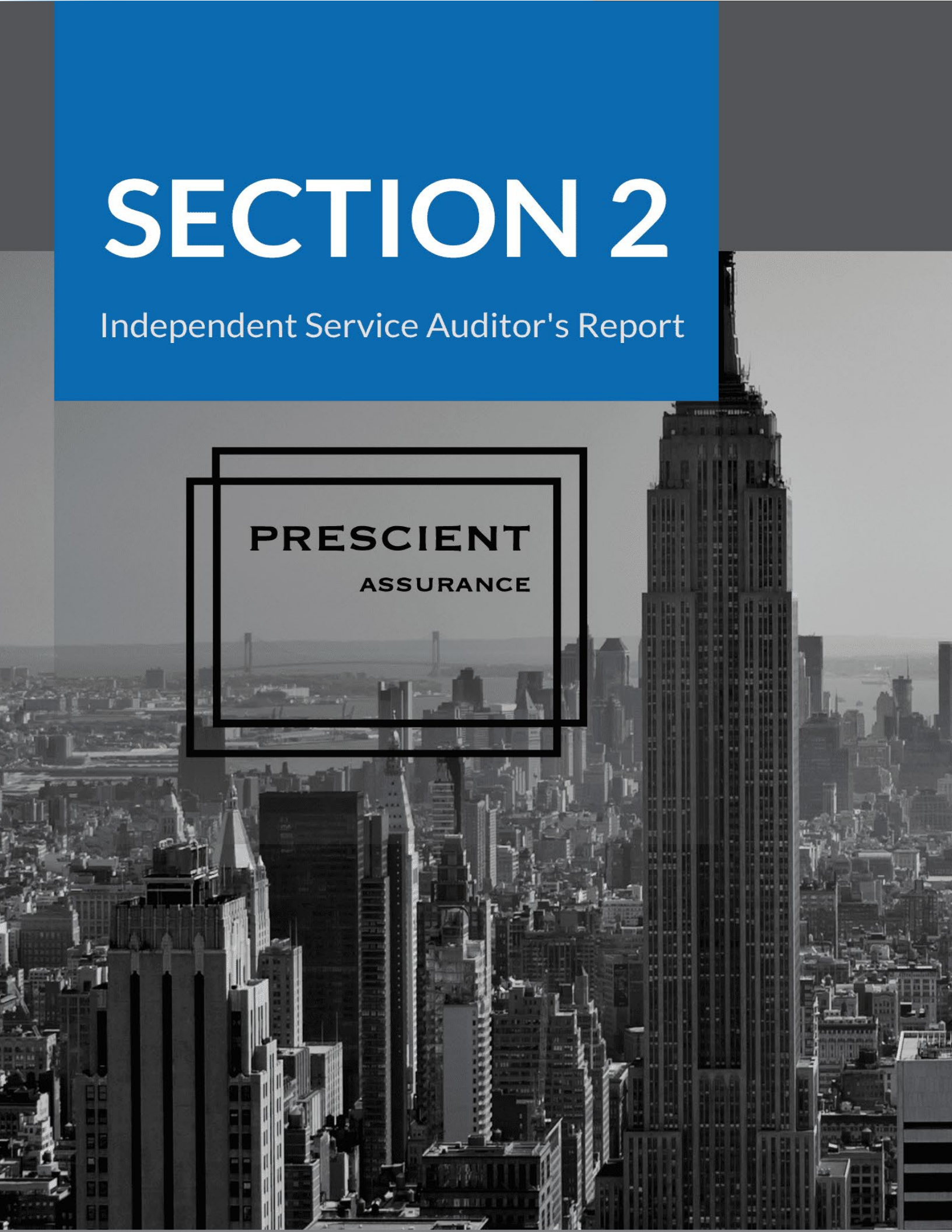
Amit Kothari
CEO
Tallyfy, Inc.



SECTION 2

Independent Service Auditor's Report

PRESCIENT
ASSURANCE



Independent Service Auditor's Report

To: Tallyfy, Inc.

Scope

We have examined Tallyfy, Inc.'s ("Tallyfy, Inc.") accompanying description of its Tallyfy system found in Section 3, titled Tallyfy, Inc. System Description throughout the period May 21, 2024, to August 21, 2024, 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 and operating effectiveness of controls stated in the description throughout the period May 21, 2024, to August 21, 2024, to provide reasonable assurance that Tallyfy, 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*.

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

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Tallyfy, Inc., to achieve Tallyfy, Inc.'s service commitments and system requirements based on the applicable trust services criteria. The description presents Tallyfy, Inc.'s controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Tallyfy, Inc.'s controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

Service Organization's Responsibilities

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

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

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 or did not operate effectively.
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 to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
5. Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
6. 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. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects:

- a. The description presents Tallyfy, Inc.'s system that was designed and implemented throughout the period May 21, 2024, to August 21, 2024, in accordance with the description criteria.
- b. The controls stated in the description were suitably designed throughout the period May 21, 2024, to August 21, 2024, to provide reasonable assurance that Tallyfy, Inc.'s service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Tallyfy, Inc.'s controls throughout the period.
- c. The controls stated in the description operated effectively throughout the period May 21, 2024, to August 21, 2024, to provide reasonable assurance that Tallyfy, Inc.'s service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of Tallyfy, Inc.'s controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of Tallyfy, Inc., user entities of Tallyfy, Inc.'s system during some or all of the period May 21, 2024 to August 21, 2024, business partners of Tallyfy, 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, subservice organizations, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
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.

Signed by:

Prescient Assurance LLC

-----989A7EAD0D11432-----

Prescient Assurance LLC

August 29, 2024

SECTION 3

System Description



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

Company Background

Tallyfy was established in 2014 and is located in St. Louis, MO. Our mission is to enable businesses to streamline their operations by providing a workflow platform that helps automate and track business processes, documents, forms and approvals. Our software helps users document any repeatable processes, launch it whenever required and track progress of every workflow in real-time. Our platform is used around the world by companies in multiple industries and with varying security program maturity.

Overview of the System (or Service or Product)

Tallyfy provides a platform that helps companies document, track and launch workflows - in order to track their status. This helps people avoid the time wasted with manual status updates, digitizing forms and information as well as automating the handover of tasks between people or teams. Tallyfy helps automate all kinds of workflows which involve tasks between people - such as client onboarding, employee orientation, financial approvals, marketing approvals and digitizing playbook templates.

Tallyfy provides a secure URL at <https://go.tallyfy.com> where people can use the platform. This system is designed to allow customers to document any procedure or process, such that anyone can launch a process to “rinse and repeat” that documented processes - without any need to re-invent the wheel for repeatable processes. Tallyfy also helps customers input their business processes into our product. In some cases, Tallyfy can save up to 1 hour per person, per day - which was previously wasted on busywork like manual meetings, chats or spreadsheet updates.

Key Features of Tallyfy

Tallyfy is comprised of the following key features:

- **Template Editor** - this feature allows customers to create a template of a blueprint, which is either a procedure, a form or a document. A blueprint is the single master template that will be launched into many processes. You can share a blueprint publicly to anyone with the link, and it can also be shared and publicized within our public blueprint library.
- **Launch Process** - the ability to launch a process via a blueprint, for specific and tailored tracking of a workflow.
- **Tracker** - the ability to track every workflow and the status of that workflow at a high-level. You can also decide to share a specific task in a process to a guest - which is any email address outside your company. An entire process can also be shared to anyone with a link, in read-only mode. Within the tracker, you can build custom views to only see the processes you want.
- **Tasks** - the ability to see a view of all tasks assigned to you or someone else, across all processes in the system. You can also see tasks assigned to guests - who are users outside your company.
- **Reminders and Settings** - the ability to customize reminders and other settings to suit individual needs. Guests (outside the company) can also tailor their reminder email settings and cadences.

DC 2: The Principal Service Commitments and System Requirements

Tallyfy has designed its processes and procedures related to the workflow platform (or the “System”) to meet its objectives for customers to document and run workflows (“Services”). Those objectives are

based on the service commitments that Tallyfy makes to user entities and the operational and compliance requirements that it has established for the services. Tallyfy's services are subject to the security requirements of security laws and regulations in the jurisdictions in which Tallyfy services are offered. This report is limited in scope to the Security Trust Services Criteria based on guidance from the AICPA.

Security commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online. Security commitments are standardized and include, but are not limited to, the following:

- Use of encryption technologies to protect data both at rest and in transit
- Network segmentation to ensure that customer data is not shared with other customers
- Official HSTS compliance of our domain tallyfy.com to ensure we always load over https, not http
- Automatic rate limiting and dynamic web application firewalls managed by Cloudflare
- Country-based blocks that prevent IP's from trade-sanctioned countries from accessing Tallyfy
- High sensitivity firewalls and limits for our dedicated sub-domain account.tallyfy.com to ensure registrations and logins are well-protected.
- Free SSO (single sign on) with a range of common identity providers to strongly encourage customer adoption of delegated authentication.
- Automatic blocking of weak cipher suites - with a minimum of TLS v1.2 required.
- Automatic blocking of traffic that comes from Tor exit nodes.

Tallyfy establishes operational requirements that support the achievement of security commitments, relevant laws and regulations, and other system requirements. Such requirements are communicated in Tallyfy's system policies and procedures, system design documents, and contracts with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed and how employees are hired and trained. In addition to these policies, standard operating procedures have been documented on how to carry out specific manual and automated processes required in the operation and development of our workflow platform.

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

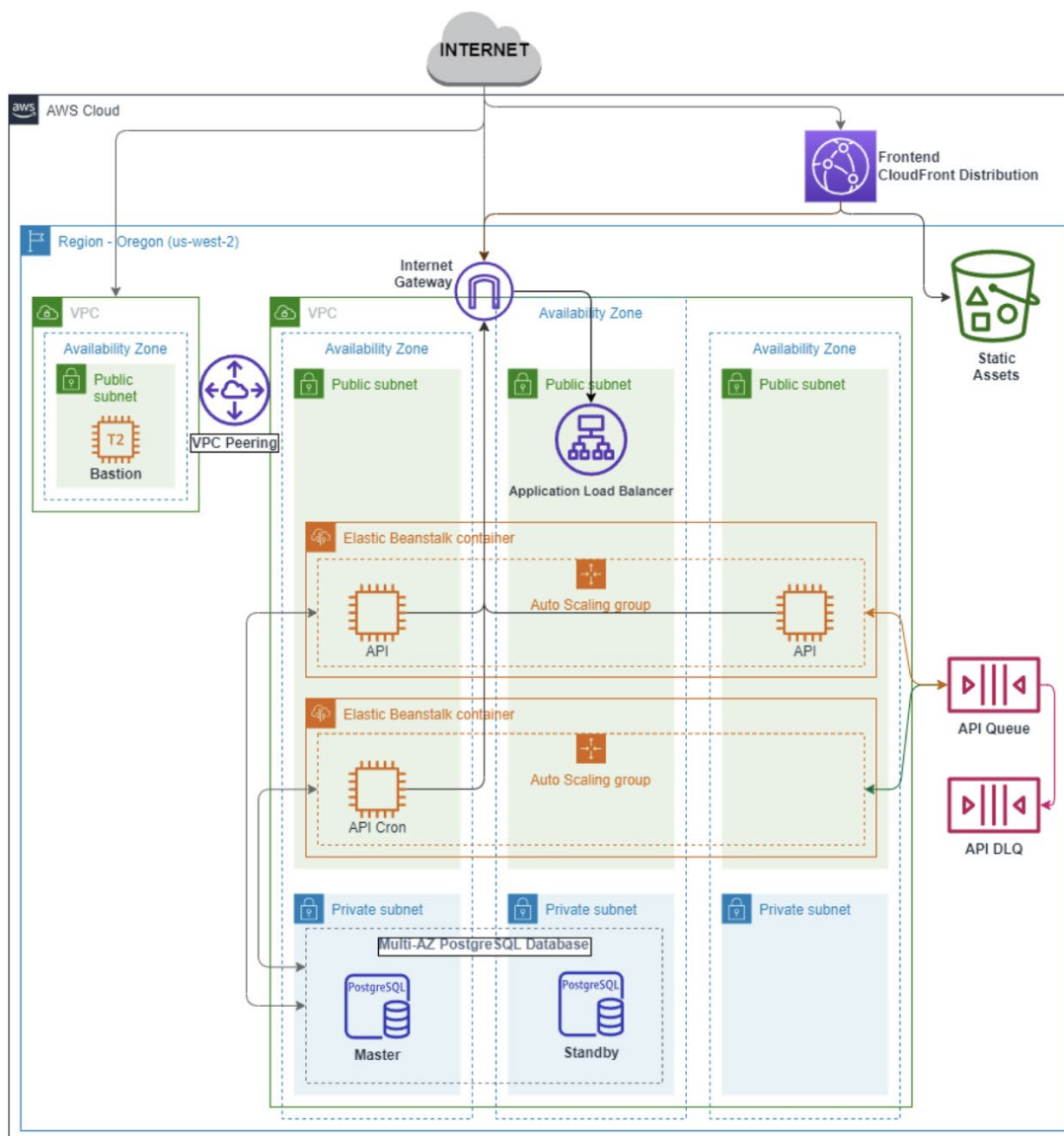
The Tallyfy platform is designed, implemented, and operated to achieve specific business objectives in accordance with management-specified requirements. The purpose of this system description is to delineate the boundaries of the system, which includes the services outlined above and the following components, described below: people, data, infrastructure, software, and processes.

The boundaries of the Tallyfy system include applications and infrastructure that directly support the services provided to Tallyfy customers. Any applications, databases, and infrastructure that indirectly support the services provided to Tallyfy customers are not included within the boundaries of the system.

3.1 Primary Infrastructure

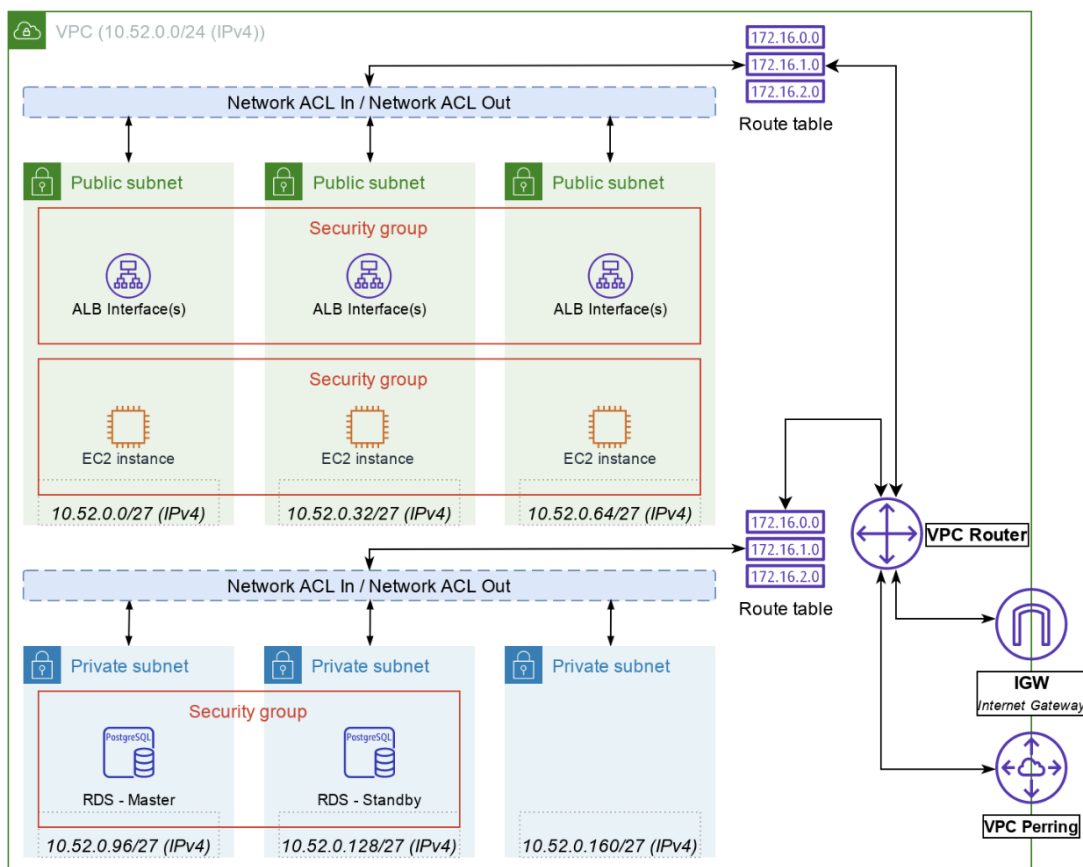
The primary infrastructure supporting Tallyfy is comprised of:

AWS Computing Infrastructure		
Infrastructure	Type	Purpose
AWS RDS	Database	Primary production database
AWS IAM	Network	Identity management
AWS S3	Storage	Simple file storage
AWS GuardDuty	Threat Detection Tool	Intelligent Threat Detection
AWS EC2 and EBS	Compute	Compute and processing servers
AWS CloudWatch	Monitoring Tool	Monitors systems and logs events
AWS SQS	Queues	Simple queues for background jobs



Tallyfy V2 Infrastructure

Network Diagrams



A general network diagram representing the configuration of the VPC network together with the security layer.

3.2 Primary Software

Tallyfy relies on the following software tools to secure and manage the System :

Software	Purpose
GitHub	Source code, backup, version control
Deploybot	Config and deployment service
Google Drive	Document management

3.3 People

Tallyfy is organized into functional areas. Within these functional areas, organizational and reporting hierarchies have been defined, and responsibilities have been assigned. Responsibilities for specific roles are clearly defined with job descriptions. The organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled and monitored.

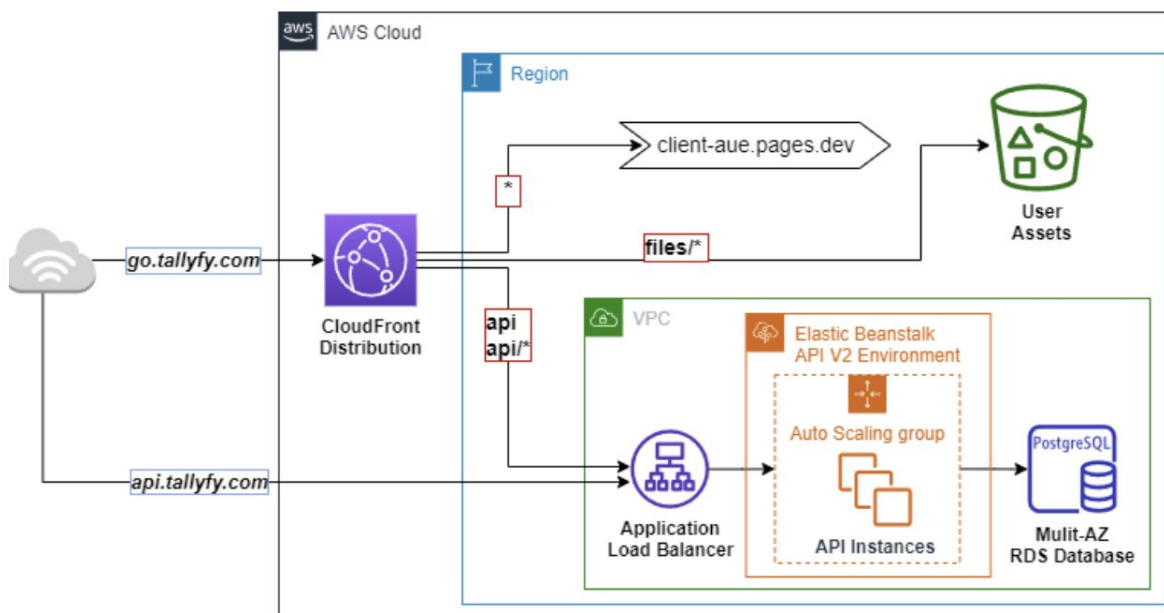
- **Leadership and Product Management:** responsible for setting the company's strategic goals and managing company-wide activities, and the product roadmap.
- **API engineering:** responsible for developing features and supporting the API.
- **Client engineering:** responsible for developing features and supporting the client user interface.
- **Human Resources (HR):** responsible for HR policies, practices, and processes (e.g. talent acquisitions, compensation, employee benefits, employee compliance, onboarding, offboarding and training).

3.4 Data

Tallyfy separates customer data using a logical permission scheme. Access to data is dependent upon the email domain and organization ID that for the user's account be validated. In this method all data for the users of an orgID (defined by a UUID) are logically separated from other orgID's within the System.

Only the Tallyfy CEO and senior engineering managers have access to production data. All customer data in the system, whether sensitive or standard, is encrypted both at transmission and at rest.

Tallyfy retains data on a case-by-case basis which is specified in a customer's contract. In the event that data is needed to be destroyed this must be approved by the CEO and a ticket provided for that removal. A backup must be made before any data is destroyed. Then the after-action activity must include a test and review by the customer that the data was properly destroyed.



Tallyfy collects and utilizes the following data elements:

Data Element (and Use)	Classification	Necessity
Email Address (Authentication & Identification)	Sensitive	Required
Password (Authentication & Identification)	Sensitive	Required
Risk Object <ul style="list-style-type: none">• Risk Name• Risk Description• Associated Controls• Score• Risk Owner	Standard	Not Required
Control Object <ul style="list-style-type: none">• Control Name & Description• Associated Security Criteria• Associated Risk• Associated Evidence• Control Owner	Standard	Not Required
Evidence Object <ul style="list-style-type: none">• Evidence Name & Description• Associated Control• Attachments	Standard	Not Required

Tallyfy classifies data into two categories: Sensitive and Standard. Sensitive data elements include passwords. Sensitive data elements are always restricted in terms of access and masked in presentation to the end users. Such elements are also never stored in clear-text in our database.

3.5 Processes and Procedures

Both automated and manual processes have been established by the organization to support the operations of Tallyfy. These include procedures through which services activities are initiated, authorized, performed, and delivered. Management has developed policies that establish the organization's overall approach to internal controls related to security and operational processes. These policies comply with overall business objectives and are aimed to minimize risk through preventive measures, timely identification of irregularities, limitation of losses, and timely restoration.

The organization's policies include the definition of assignment responsibilities and address the following security life cycle processes which are further described in the Control Environment section of this document:

- Oversight, selection, documentation, implementation and monitoring of security controls
- Authorization, changes to, and termination of information system access
- Maintenance and support of the security system and necessary backup and offline storage
- Governance and processes for change management
- Incident response guidelines and processes including annual table top exercises
- Vendor oversight and processes to mitigate vendor risk
- IT and operational risk management including annual business continuity tests
- Privileged access reviews annually
- Annual performance reviews
- Annual penetration tests
- Annual vulnerability scans

3.6 Third Party Access

Staff at AWS have access to our hosted network. This provider does not have access to any client databases.

DC 4: Disclosures About Identified Security Incidents

There have been no reported incidents in the 12 months prior to the end date of the audit period covered by this report.

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

Control Environment

Tallyfy's control environment sets the tone of the organization and influences the control consciousness of its personnel. Some of the components of internal control include controls that have more of an effect at the entity level, while other components include controls that are primarily related to specific processes or applications. The control environment includes controls that may have a pervasive effect on the organization, an effect on specific processes, as well as security controls intended to effectively protect client data and provide a stable environment for the security of Tallyfy's client-facing services. The components of the control environment factors include the integrity and ethical values, management's commitment to competence; its organizational structure; the assignment of authority and responsibility; and the oversight and direction provided by leadership.

5.1 Integrity and Ethical Values

Integrity and ethical values are essential elements of Tallyfy's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Tallyfy's ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. Specific items that Tallyfy has implemented in this area are:

- NDA
- Code of Conduct
- Employee Performance Review
- Acceptable Use Policy

5.2 Management Oversight

Management Oversight - Tallyfy's control consciousness is influenced significantly by the participation of its executive team. The executive team meets on a periodic basis to oversee operations management activities and to discuss and monitor related issues. Executive management meets and interacts with team members as a component of day-to-day operations to discuss business objectives and operational issues.

Tallyfy's control consciousness is influenced significantly by the participation of its executive team. The executive team meets on a periodic basis to oversee operations management activities and to discuss and monitor related issues. Executive management meets and interacts with team members as a component of day-to-day operations to discuss business objectives and operational issues.

5.3 Organizational Structure

Tallyfy organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Tallyfy management believes that establishing a relevant organizational structure includes considering key areas of authority and responsibility and lines of reporting. Tallyfy is organized along functional areas. Within functional areas, organizational and reporting hierarchies have been defined and responsibilities have been assigned.

5.4 Assignment of Authority and Responsibility

Tallyfy's assignment of authority and responsibility 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 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 that 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.

5.5 Commitment to Competence

Tallyfy is committed to providing the highest quality professional and technological resources. This includes management's consideration of the knowledge and skills necessary to accomplish tasks that define each employee's roles and responsibilities. To this end, management has implemented the following:

- Job Descriptions
- Business Continuity Plan
- Logical Access
- Role Based Access
- Vendor Management Expectations
- Incident Response
- Non Disclosure Agreement
- Acceptable Use Policy
- Code of Conduct
- Employee Performance
- Security Training
- Separation of Duties - Developers

5.6 Accountability

Tallyfy management philosophy and operating style encompass a broad range of characteristics. Such characteristics include management's approach to taking and monitoring business risks, management's attitudes and actions toward financial reporting, and management's attitudes toward information processing, accounting functions and personnel. Management meetings are held frequently to address issues as they are brought to management's attention. Tallyfy' human resources policies and practices relate to employee hiring, orientation, training, evaluation, promotion, compensation, and disciplinary activities. Specific items that Tallyfy has implemented in this area include:

- Code of Conduct
- Job Descriptions
- Employee Performance
- Separation of Duties - Developers
- Security Training

5.7 Security Management

Management has developed information security policies and related procedures to govern the security program at Tallyfy. The Information Security Policy is maintained, reviewed and annually updated by the CEO. The development of an information security program, processes and procedures are the responsibility of the CEO. The Information Security Policies are reviewed and approved annually or as business needs change. Procedure documents related to access control and change management are updated as business needs change.

These policies and procedures cover the following key security life cycle areas:

- Data classification

- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response

Logical Access

- The policy and procedures for logical access are owned by the CEO.
- Assets are classified as privileged access, vendor access, emergency access and temporary access.
- Upon hire, a designated Manager notifies the CEO, providing the new user's name, email alias (if it will vary from the standard alias), and the security settings to be used. Access to software (GitHub, AWS, etc.) is provisioned by the application owner, based on the principle of least privilege. Documentation of provisioning should be within a ticket in the ticketing system or within the Tallyfy onboarding process.
- Modifications to access must be approved by an authorized employee. The Network Team will only process access requests and modifications when granted by an authorized employee. Modifications should be documented within a ticket.
- Sensitive systems such as our database holding production data is only accessible to the CEO and 2 Technical Team Leads - the API and client team lead.
- Passwords for all systems (critical network, tools, operating systems, databases, applications, VPNs) must adhere to the following settings:
 - Strong passwords are enforced where feasible
 - Complexity is enforced by requiring lowercase letters, uppercase letters, numbers, and special characters
- Critical systems require access via Cloudflare Zero Trust or AWS IAM, which include MFA.
- All Tallyfy engineers and workers may use their own devices to work, and access control is run at the network level via IAM and Cloudflare Zero Trust. All applications are cloud-based and secured via access control using Cloudflare Zero Trust.
- We use a default, managed firewall via Cloudflare.

Tallyfy employees all currently work from remote locations. Tallyfy is generally located in the St. Louis, MO area but due to the global pandemic all employees work from home. Tallyfy employees utilize encrypted communications and locally encrypted hard drives to ensure sensitive non-customer data is secured. Tallyfy policies and controls do not tolerate the use of customer data outside of Amazon Web Services.

Tallyfy does not retain any customer data, sensitive information or property at any physical location. Since all of Tallyfy's risk sensitive business is conducted in the cloud, access is carefully secured via IAM policies on Amazon Web Services. Tallyfy relies on the physical access controls provided by Amazon Web Services to ensure servers, hard drives and networking equipment is carefully secured in their data center.

Change Management

Tallyfy has a Change Management Policy which governs deliberate changes to the IT environment, including infrastructure, data, and software development. The Change Management policy governs the request, documentation, testing and approval of changes. All technology acquisition, development and maintenance processes are governed by change management procedures. The Change Management Policy is communicated to relevant personnel and updated annually, or as business needs require. The CEO is the owner of the Change Management Policy and is responsible for ensuring that changes to IT services are made in a manner appropriate to their impact on Company Operations.

Tallyfy has implemented a SCRUM based software development lifecycle as a change management practice. We design our release roadmap around enhancement releases, minor releases and major releases. Prioritization is the responsibility of the CEO.

Tallyfy's product team utilizes GitHub to manage specific changes throughout the change control processes. For any system change a ticket must be written specifying the change requested. Tallyfy's CEO elicits prioritization of the ticket with the team leads for API and client.

When tickets have been prioritized they are matched with a planned software release. A release will include multiple tickets. Enhancement releases can be accomplished the most quickly and can include important bug fixes and patches when threats arrive. Minor releases usually correspond with a new feature. Major releases can contain multiple features or new products unto themselves. A release is identified then prioritized tickets are then assigned to it.

Weekly Sprint Planning meetings allow the Product Manager to assign specific tasks according to the release roadmap. This also provides an important touchpoint for the entire product team. Standup meetings three times a week with the team allow for quick decisions or questions to be introduced during a sprint.

Executed changes are developed in software code on a separate branch of a project's git repository. When an engineer or resource has completed a ticket in their separate branch they create a "merge request" in the git repository. A merge request must be reviewed and approved by a separate engineer or resource. Once the request has been approved the merge request can be completed and the software code is included in a development branch within the git repository. The developer branch is automatically deployed via Deploybot CI/CD tools to the development environment on AWS. This environment allows the product team to execute rapid tests in the complete merged code base on a duplicated server environment.

Once the required tickets for a specific release are completed the development branch is merged to a staging branch. This is executed with the approval of the API or client team leads. Staging branches are automatically deployed to a staging environment on AWS that is duplicated via CloudFormation to the production environment. This allows the product team to execute a complete regression test for a possible production release. Throughout this process ONLY the production environments may hold customer data, therefore the data in staging and development environments are created by testers.

After a regression test has been completed and the quality of the code approved by the CEO a production release can be created. The Tallyfy API or client team lead tags the staging branch with a tag that specifies the release number e.g. 1.1.0. This tag is then pushed via command through the Deploybot process registering the code and then deploying that code to Elastic Beanstalk. The CEO and engineering team leads then perform a brief smoke test to ensure that the changes have not resulted in an error. If any roll-back activity is required the CEO or engineering team leads will execute that immediately.

Emergency change requests follow the same process as other change requests - but they do not always need a second independent approver to merge and push to production.

In this way Tallyfy carefully ensures that changes are planned, orchestrated, tested and released in predictable patterns.

Data Backup and Disaster Recovery

All Tallyfy customer data is considered the highest priority for data retention. Our databases are deployed on the Relational Data Service (RDS) provided by Amazon Web Services. Our database software provides full ACID compliant transaction support. Every database has an automated data backup and restoration policy. This is coded into CloudFormation deployment scripts and tested with each major release. Backups are achieved using AWS tools daily and all snapshots are retained for 30 days. Data is backed up following a set schedule; access to backups is restricted to privileged users.

For added security Tallyfy retains important software characteristics with the concurrent versioning system Git hosted by GitHub.com.

In the event of a catastrophic disaster where the database in its entirety is down and requires complete rebuilding from the ground up, Tallyfy Engineers will follow a documented and tested restoration process. Tallyfy has a Disaster Recovery Plan that is tested when significant changes to procedures invalidate previous testing.

Incident Response

Tallyfy relies on AWS' incident logging system for incidents impacting the AWS infrastructure. For other incidents, incident response guidelines are published and available to all employees and include definition of an incident, employee responsibilities and notification procedures, and data necessary to analyze an incident to determine impact are documented. A security incident recovery test is performed annually; resulting findings are integrated into the Security Incident Response Plan ("SIRP").

The SIRP includes:

- definition of an incident
- employee responsibilities
- notification procedures
- containment
- mitigation plan
- a step to apply patch, fix, restoration of data, or enable new tool setting (such as firewall rules)
- restoration of services
- root cause analysis

A tracking system is in place to centrally maintain, manage, and monitor change requests that result from incidents that require a change to be made. Incident response procedures for all employees are included in the annual security training.

Vendor Management

The organization clearly defines vendor management roles, contract expectations and vendor risks in adherence to their Vendor Management Policy. Vendor management is overseen by the CEO. Formal contracts are utilized for vendor and business partner relationships; scope, responsibilities, compliance requirements and service levels (if required) are included in the contracts.

Tallyfy performs due diligence activities over new vendors prior to contract execution and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk. Third party SOC 2 reports are reviewed for impact to the company environment.

System Monitoring

The Tallyfy platform is monitored on both the infrastructure level and the application level. Tallyfy utilizes an infrastructure/application monitoring tool (CloudWatch) to detect abnormalities in the application and monitor SLAs. Notifications are monitored by the Engineering Team and all alerts, depending on their criticality, will notify appropriate users through a combination of email or Slack messaging.

A cloud monitoring tool is utilized to log changes to cloud services and audited on an as needed basis.

Antivirus software is deployed to information systems. AWS employs firewall solutions.

5.8 Information and Communications

Information and communication is an integral component of the Tallyfy internal control system. It is the process of identifying, capturing and exchanging information in the time frame necessary to conduct, manage and control the entity's operations. At Tallyfy, information is identified, captured, processed and reported by various information systems, as well as through conversations with clients, service providers, and employees.

Standups are held three times a week to discuss the status of the current sprint activities which may include security tasks. Departmental meetings are utilized to align team objectives with company objectives. Engineering and the CEO converse on our chat platform weekly to look back on all on-call and security alerts triggered over the previous week. Additionally, company wide meetings are held weekly to disseminate new policies, procedures, controls and other strategic initiatives within the organization. The company document management system includes information employees can reference for data security guidance. Additionally, email and Slack messages are used to communicate time-sensitive information.

Tallyfy has also implemented various methods of communication to help provide assurance that customers understand their roles and responsibilities in processing their data and communication of significant events. This includes a dedicated support team to communicate time-sensitive information when there are customer impacting security changes. Customer Support will notify customers of maintenance, outages, product releases, security incidents or platform changes that negatively impact security or privacy. External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the Support webpage. The incident is documented in accordance with the Incident Response Plan.

5.9 Monitoring

Monitoring is a critical aspect of internal control in evaluating whether controls are operating as intended and whether they are modified as appropriate for changing conditions. Management has implemented monitoring controls to address timely and appropriate responses to issues that may impact information security. Automated systems (ex: IDS, firewall, vulnerability scans, patch alerts) are monitored for security events impacting Company systems and remediations are actioned as needed.

In addition, Management monitors the quality of internal control performance as a normal part of their activities. They are heavily involved in day-to-day activities and regularly review various aspects of internal and customer-facing operations to:

1. Determine if objectives are achieved
2. Identify any new risks that develop
3. Implement appropriate measures to address those risks

The monitoring process is achieved through several ongoing management oversight activities that include the assessment of audit results performed by independent auditors.

5.10 Risk Assessment

Management is responsible for identifying risks that threaten achievement of the control activities stated in the management's description of the services organizations systems. Management has implemented a process for identifying relevant risks that could affect the organization's ability to provide secure and reliable service to its users. The risk assessment occurs annually, or as business needs change, and covers identification of risks that could act against the company's objectives as well as specific risks related to a compromise to the security of data.

The level of each identified risk is determined by considering the impact of the risk itself and the likelihood of the risk materializing and high scoring risks are actioned upon. Risks are analyzed to determine whether the risk meets company risk acceptance criteria to be accepted or whether a mitigation plan will be applied. Mitigation plans include both the individual or department responsible for the plan and may include budget considerations.

Management considers the following in its risk assessment:

- Risks that could impact the security of the organization's IT environment
- Cross department risks that may impact security objectives
- Identification and assessment of changes, such as environmental, regulatory, and technological changes that could significantly affect the system of internal control for security
- Development and implementation of mitigation strategies for those risks

DC 6: Complementary User Entity Controls (CUECs)

Tallyfy's services were designed with the assumption that certain controls would be implemented by user-entities. These controls should be in operation at user entities to complement Tallyfy's controls. The user-entity controls subsequently presented should not be regarded as a comprehensive list of all controls that should be employed by user-entities:

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

The cloud hosting services provided by AWS were not included within the scope of this examination.

The following table presents examples of applicable Trust Services criteria that are intended to be met by controls at our sub-service providers, alone or in combination with controls at Tallyfy, and the types of controls expected to be implemented by our sub-service providers to meet those criteria.

Control	Applicable Trust Services Criteria
AWS is responsible for ensuring network protection for the cloud environment through the use of a proprietary hypervisor firewall and security monitoring applications that are configured and monitored by AWS personnel.	CC 4.1 CC 4.2 CC 6.6 CC 6.8
AWS is responsible for server patch management.	CC5.2
AWS is responsible for managing logical access to the underlying network, virtualization management, and storage devices for its Infrastructure as a Service ("IaaS") cloud hosting services where Company systems reside.	CC 6.1
AWS is responsible for ensuring physical access restriction to the facilities, offline storage and backup data, monitoring network, and other system components such as firewalls, routers, and servers.	CC 6.4
AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the server rooms.	CC7.2
AWS is responsible for protecting the server rooms against disruption in power supply to the processing environment by an uninterruptible power supply.	CC7.2
AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.	CC7.2

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria

All security were relevant and applicable to the platform as detailed in this report.

DC 9: Disclosures of Significant Changes in Last 1 Year

There have been no significant changes within the last 12 months.

SECTION 4

Testing Matrices

PRESCIENT
ASSURANCE

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Tallyfy provided by Tallyfy, Inc.. The scope of the testing was restricted to Tallyfy, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period May 21, 2024 to August 21, 2024.

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

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: <ul style="list-style-type: none">• Examination / Inspection of source documentation and authorizations to verify transactions processed.• Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures.• Examination / Inspection of systems documentation, configurations, and settings; and• Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.

Test Types	Description of Tests
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System-generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

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

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase "No exceptions noted." in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	COSO Principle	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	A formal performance evaluation procedure is in place and employees are evaluated at least annually.	Inspected evidence of performance evaluations performed for a sample of current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.	Inspected the Vendor Management Policy and vendor list to determine that the company clearly defines and documents vendor management roles, contract expectations and vendor risks.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	Due diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	Inspected compliance reports, risk assessment, and reviews to determine that the company implements Due diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter, this includes an assessment of information security practices based on the assessed level of vendor risk.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	A code of conduct exists and is required to be signed by all employees upon hire. The code of conduct is updated by management as needed, and available to employees via the human resources site.	<p>Inspected the Code of Conduct Policy to determine that the company's management updates the Code of Conduct as needed and is accessible to employees through a shared drive.</p> <p>Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.</p>	<p>No exceptions noted.</p> <p>Not tested. There were no new hires during the audit period</p>
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The role has been formally assigned for oversight of information security and primary business practices. The assignee communicates the importance of effective information security management and of conforming to the information security management system requirements.	Inspected the Information Security Policy and CEO Linked In profile to determine that a role is assigned to oversee information security and business practices. Verified that this role ensures effective management and compliance with system requirements.	No exceptions noted.
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and	The management has sufficient expertise to oversee internal controls.	Inspected the bio's of company management to determine that the company's management has sufficient expertise to oversee internal controls.	No exceptions noted.

	performance of internal control.			
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	Inspected a sample of job descriptions to determine that the company has job descriptions in place which define the skills, responsibilities for specific roles, include responsibility as they relate to information security and are available to all employees	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.	Inspected the Vendor Management Policy and vendor list to determine that the company clearly defines and documents vendor management roles, contract expectations and vendor risks.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The new hire screening process includes a consideration of skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are also performed prior to hire.	Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	Not tested. There were no new hires during the audit period
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	Inspected a sample of job descriptions to determine that the company has job descriptions in place which define the skills, responsibilities for specific roles, include responsibility as they relate to information security and are available to all employees	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	A formal performance evaluation procedure is in place and employees are evaluated at least annually.	Inspected evidence of performance evaluations performed for a sample of current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain	Due diligence activities are performed over new vendors prior to contract execution, and	Inspected compliance reports, risk assessment, and reviews to determine that the company implements Due	No exceptions noted.

	competent individuals in alignment with objectives.	on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter, this includes an assessment of information security practices based on the assessed level of vendor risk.	
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	A formal performance evaluation procedure is in place and employees are evaluated at least annually.	Inspected evidence of performance evaluations performed for a sample of current employees to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Employees complete security related training, as relevant to their duties, upon hire and on an annual basis. The annual security training includes information on how to report security incidents and concerns.	Inspected a sample of employee completed security tasks to determine that the company has Employees complete security related training, as relevant to their duties on an annual basis, and includes information on how to report security incidents and concerns. Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	No exceptions noted. Not tested. There were no new hires during the audit period.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	Inspected compliance dashboard to determine that the company's internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies. Inquired with company management to determine that there were no identified deficiencies during the audit period.	No exceptions noted. Not tested. There were no identified deficiencies during the audit period.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Control deficiencies and results of separate evaluations are communicated to, and monitored by the CEO and other senior management, as appropriate. Security and IT operational issues are tracked and monitored.	Inquired of company management to determine that there were no deficiencies identified during the audit window.	Not tested. There were no deficiencies identified during the audit window.
CC2.1	The entity obtains or generates and uses relevant,	An annual risk assessment is conducted to identify, assess,	Inspected the risk assessment to determine that the company conducts	No exceptions noted.

	quality information to support the functioning of internal control.	mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The design, implementation, maintenance, execution, and annual of the security incident response program and data breach response procedures are the responsibility of the CEO.	<p>Inspected the Information Security Policy and Disaster Recovery and Business Continuity Plan to determine that the security incident response program and data breach response procedures are the responsibility of the CEO.</p> <p>Inspected the tabletop exercise to determine that the company security incident response program and data breach response procedures are tested at least annually.</p>	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.	Inspected the data flow diagram to determine that it is maintained and highlights the systems requiring logical access controls based on data classification levels.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	Inspected the network diagram to determine that the company boundaries are defined and is reviewed annually or as business needs require.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The organization utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers; scope, responsibilities, compliance requirements, and service levels are included in the contract.	Inspected the customer service agreement to determine that the company utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	External parties may report systems failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in	Inspected the contact page to confirm that external parties can report system failures, incidents, concerns, and other complaints by submitting their issues via the organization's support webpage.	No exceptions noted.

		accordance with the Incident Response Plan, if required.	Inquired of company management to determine that there were no security incidents during the audit period.	Not tested. There were no security incidents during the audit period.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.	Inspected the Security Incident Response Policy and Plan to determine that the company has a documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. Inspected the Breach Template to determine that the company has a process in place to address data breaches.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	A centralized drive is in place for employees to access all corporate policies and procedures as well as job descriptions.	Inspected the drive records to determine employee access to policies and procedures as well as job descriptions.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	All employees are required to acknowledge the Acceptable Use Policy upon hire. The policy outlines rules for the acceptable use of information associated with information and information processing, as well as, appropriate procedures for compliance with legislative, regulatory, and contractual requirements related to proprietary software services. The policy is updated by management as needed and available to employees.	Inspected the Acceptable Use Policy to determine that the company outlines rules for the acceptable use of information and information processing, as well as, appropriate procedures for compliance. Inspected the Acceptable Use Policy to determine that the company's management updates the Acceptable Use Policy as needed and is accessible to employees through a shared drive. Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	No exceptions noted. No exceptions noted. Not tested. There were no new hires during the audit period.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Employees complete security related training, as relevant to their duties, upon hire and on an annual basis. The annual security training includes information on how to report security incidents and concerns.	Inspected a sample of employee completed security tasks to determine that the company has Employees complete security related training, as relevant to their duties on an annual basis, and includes information on how to report security incidents and concerns. Inquired of company management	No exceptions noted.

			and inspected the access reviews to determine that there were no new hires during the audit period.	Not tested. There were no new hires during the audit period.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	Inspected a sample of job descriptions to determine that the company has job descriptions in place which define the skills, responsibilities for specific roles, include responsibility as they relate to information security and are available to all employees	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	Inspected compliance dashboard to determine that the company's internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies. Inquired with company management to determine that there are no identified deficiencies during the audit period.	No exceptions noted. Not tested. There were no identified deficiencies during the audit period.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers; scope, responsibilities, compliance requirements, and service levels are included in the contract.	Inspected the customer service agreement to determine that the company utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	External parties may report system failures, incidents, concerns, and other complaints to appropriate personnel by submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required.	Inspected the contact page to confirm that external parties can report system failures, incidents, concerns, and other complaints by submitting their issues via the organization's support webpage. Inquired of company management to determine that there were no security incidents during the audit period.	No exceptions noted. Not tested. There were no security incidents during the audit period.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective	Inspected compliance dashboard to determine that the company's internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies.	No exceptions noted.

		action plan, and communicating them to management for review.	Inquired with company management to determine that there are no identified deficiencies during the audit period.	Not tested. There were no identified deficiencies during the audit period.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.	Inspected the penetration test report to determine that the company contracts an independent third-party provider to perform penetration tests at least annually and, test results are reviewed and tracked to resolution.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.	Inspected the Vendor Management Policy and vendor list to determine that the company clearly defines and documents vendor management roles, contract expectations and vendor risks.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.	Inspected the Security Incident Response Policy and Plan to determine that the company has a documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. Inspected the Breach Template to determine that the company has a process in place to address data breaches.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	Inspected critical SOC 2 report and review to determine that the company maintains critical third-party SOC 2 reports and reviews are formally documented by management.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Risk assessment policy and procedures are in place and include how to identify risks, to evaluate risks, and how to address and mitigate those risks.	Inspected the Risk Management Policy and risk assessment to determine that the company's risk assessment policy and procedures are in place and include how to identify, evaluate, address, and mitigate risks.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and	Risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned	Inspected annual risk assessment to determine that the company risks are identified through a risk assessment process, addressed by management, and appropriate mitigation strategies	No exceptions noted.

	assessment of risks relating to objectives.	and tracked for completion. Risk treatment activities are documented accordingly.	or risk acceptance are assigned and tracked for completion.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion. Risk treatment activities are documented accordingly.	Inspected annual risk assessment to determine that the company risks are identified through a risk assessment process, addressed by management, and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	Inspected the network diagram to determine that the company boundaries are defined and is reviewed annually or as business needs require.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality.	Inspected the Disaster Recovery and Business Continuity Plan and tabletop exercise to determine that the company has developed a Disaster Recovery and Business Continuity Plan and reviewed it in the event of a catastrophic event. The Disaster Recovery and Business Continuity Plan documents the roles & responsibilities, and milestones for maintaining business continuity and restoring system functionality.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	An inventory of information assets, including hardware, software, processing facilities and data, is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.	Inspected the Data Classification Policy to determine that the company assets are classified based on the data classification convention. Inspected Infrastructure documentation to determine that the company has an inventory of information assets (including hardware, software, and data), assets have an assigned asset owner and is updated at least annually.	No exceptions noted.

CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	A defined information classification scheme has been established to label and handle data. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, Non-public.	Inspected the Data Classification Policy to determine that an information classification scheme has been established to label and handle data and the classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	Inspected critical SOC 2 report and review to determine that the company maintains critical third-party SOC 2 reports and reviews are formally documented by management.	No exceptions noted.
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.	Inspected the data flow diagram to determine that it is maintained and highlights the systems requiring logical access controls based on data classification levels.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	Inspected critical SOC 2 report and review to determine that the company maintains critical third-party SOC 2 reports and reviews are formally documented by management.	No exceptions noted.

CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.	Inspected the penetration test report to determine that the company contracts an independent third-party provider to perform penetration tests at least annually and test results are reviewed and tracked to resolution.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	IT infrastructure monitoring tools are configured to monitor IT infrastructure availability and performance, generate alerts when specific predefined thresholds are met, and forecast capacity requirements to ensure system performance.	Inspected the monitoring and alert configurations to determine that infrastructure monitoring tools are configured to monitor IT infrastructure availability and performance, generate alerts when specific predefined thresholds are met, and forecast capacity requirements to ensure system performance.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The new hire screening process includes a consideration of skills and competencies of the candidate. Each job candidate is interviewed by personnel within the employing department to determine if education, experience, and technical competency are appropriate for the job function. Reference checks are also performed prior to hire.	Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	Not tested. There were no new hires during the audit period
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.	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	Inspected WAF configuration settings to determine that the company has a threat detection tool in place that is utilized to monitor and log possible or actual network breaches and other anomalous security events and alerts occurring on threats and results are actioned as appropriate.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the	Vulnerability scans are performed annually to help identify security risks and results	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no	No exceptions noted.

	components of internal control are present and functioning.	are triaged and actioned per Service Level Agreement.	results were triaged and actioned per Service Level Agreement.	
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.	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	Inspected compliance dashboard to determine that the company's internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies. Inquired with company management to determine that there are no identified deficiencies during the audit period.	No exceptions noted. Not tested. There were no identified deficiencies during the audit period.
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.	An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.	Inspected the penetration test report to determine that the company contracts an independent third-party provider to perform penetration tests at least annually and test results are reviewed and tracked to resolution.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	Control deficiencies and results of separate evaluations are communicated to, and monitored by the CEO and other senior management, as appropriate. Security and IT operational issues are tracked and monitored.	Inquired of company management to determine that there were no deficiencies identified during the audit window.	Not tested. There were no deficiencies identified during the audit window.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Service boundaries are defined in the network diagram. The network diagram is reviewed annually or as business needs require.	Inspected the network diagram to determine that the company boundaries are defined and is reviewed annually or as business needs require.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.

CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Developers do not have access to IT infrastructure tools or the production environment. Exceptions are documented and approved by the CEO.	Inspected users listings to determine that the developers do not have access to IT infrastructure tools or the production environment and exceptions are documented by the CEO.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	Inspected compliance dashboard to determine that the company's internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies. Inquired with company management to determine that there are no identified deficiencies during the audit period.	No exceptions noted. Not tested. There were no identified deficiencies during the audit period.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Access to the source code repository is restricted to authorized employees.	Inspected the user listings to determine that access to the source code repository is restricted to authorized employees.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Segregation of duties exist during the infrastructure and application change process, enforced in the source control system (GitHub).	Inspected user listings to determine that the company implements segregation of duties during the infrastructure and application change process and is enforced in the source control system (GitHub).	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.	Inspected the data flow diagram to determine that it is maintained and highlights the systems requiring logical access controls based on data classification levels.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	A Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality.	Inspected the Disaster Recovery and Business Continuity Plan and tabletop exercise to determine that the company has developed a Disaster Recovery and Business Continuity Plan and reviewed it in the event of a catastrophic event. The Disaster Recovery and Business Continuity Plan documents the roles & responsibilities, and milestones for maintaining business continuity and restoring system functionality.	No exceptions noted.

CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Risks identified through the risk assessment process are addressed by management and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion. Risk treatment activities are documented accordingly.	Inspected annual risk assessment to determine that the company risks are identified through a risk assessment process, addressed by management, and appropriate mitigation strategies or risk acceptance are assigned and tracked for completion.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Management performs at least an annual review of user access to systems based on job duties. Inactive users are removed and removal is documented. The review is formally documented including system generated user listings and sign off by management.	Inspected access review to determine that the company's management performs at least an annual review of user access to systems based on job duties and the review is formally documented and signed off by management. Auditor noted no changes to the access review.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.	Inspected the Logical Access Policy and Procedures, last reviewed during the audit period to determine that the company has Logical Access Policy and Procedures in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege and is reviewed annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	A Business Continuity Plan has been developed and reviewed in the event of a catastrophic event. The plan identifies a process, roles, and milestones for maintaining business continuity and restoring system functionality.	Inspected the Disaster Recovery and Business Continuity Plan and tabletop exercise to determine that the company has developed a Disaster Recovery and Business Continuity Plan and reviewed it in the event of a catastrophic event. The Disaster Recovery and Business Continuity Plan documents the roles & responsibilities, and milestones for maintaining business continuity and restoring system functionality.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Employees complete security related training, as relevant to their duties, upon hire and on an annual basis. The annual security training includes information on how to report security incidents and concerns.	Inspected a sample of employee completed security tasks to determine that the company has Employees complete security related training, as relevant to their duties on an annual basis, and includes information on how to report security incidents and concerns. Inquired of company management and inspected the access reviews to	No exceptions noted. Not tested. There were no new hires

			determine that there were no new hires during the audit period.	during the audit period.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.	Inspected the penetration test report to determine that the company contracts an independent third-party provider to perform penetration tests at least annually and test results are reviewed and tracked to resolution.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.	Inspected the Logical Access Policy and Procedures, last reviewed during the audit period to determine that the company has Logical Access Policy and Procedures in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege and is reviewed annually.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Job descriptions are in place which define the skills and responsibilities for specific roles and are available to all employees. Job descriptions include responsibility as they relate to information security.	Inspected a sample of job descriptions to determine that the company has job descriptions in place which define the skills, responsibilities for specific roles, include responsibility as they relate to information security and are available to all employees	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	IT security related policies are reviewed and approved annually or as business needs change. Procedure documents related to access control, change management, and incident management are updated as processes change.	Inspected the review dates of the System Development Lifecycle Policy, Disaster Recovery & Business Continuity Plan, and several other policies to determine that IT security-related policies are reviewed and approved annually or as business needs change.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	Inspected WAF configuration settings to determine that the company has a threat detection tool in place that is utilized to monitor and log possible or actual network breaches and other anomalous security events and alerts occurring on threats and results are actioned as appropriate.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Vulnerability scans are performed annually to help identify security risks and results are triaged and actioned per Service Level Agreement.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no results were triaged and actioned per Service Level Agreement.	No exceptions noted.
CC5.3	The entity deploys control activities through policies	Internal control responsibilities are assigned to control owners	Inspected compliance dashboard to determine that the company's	No exceptions noted.

	that establish what is expected and in procedures that put policies into action.	who are responsible for monitoring controls for deficiencies, documenting deficiencies in a corrective action plan, and communicating them to management for review.	internal control responsibilities are assigned to control owners who are responsible for monitoring controls for deficiencies. Inquired with company management to determine that there are no identified deficiencies during the audit period.	Not tested. There were no identified deficiencies during the audit period.
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.	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.	Inspected the Logical Access Policy and Procedures, last reviewed during the audit period to determine that the company has Logical Access Policy and Procedures in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege and is reviewed annually.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	All data at rest in the cloud is encrypted using industry standard algorithms.	Inspected the database configurations to determine that data at rest in the cloud is encrypted using industry standard algorithms.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Vulnerability scans are performed annually to help identify security risks and results are triaged and actioned per Service Level Agreement.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no results were triaged and actioned per Service Level Agreement.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	Logical user access requests are documented and require approval prior to access being provisioned for cloud and server systems.	Inquired of company management and inspected the access reviews to determine that there were no new hires, or requests during the audit period.	Not tested. There were no new hires, or requests during the audit period.
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.	Disk encryption is enforced on all employee devices.	Inspected a sample of hard drive encryption settings to determine that the company disk encryption is enforced on all employee devices.	No exceptions noted.

	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.	Any sensitive data that's transmitted over public networks, and data in transit is encrypted. HSTS compliance is maintained.	Inspected the encryption configurations to determine that sensitive data that's transmitted over public networks, and data in transit is encrypted, and HSTS compliance is maintained.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	A defined information classification scheme has been established to label and handle data. Classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information. Data is classified into three levels: public, confidential, Non-public.	Inspected the Data Classification Policy to determine that an information classification scheme has been established to label and handle data and the classifications consider the legal requirements, value, criticality, and sensitivity to unauthorized disclosure or modification of the information.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The data flow diagram is maintained, and highlights the systems that require logical access controls per data classification level.	Inspected the data flow diagram to determine that it is maintained and highlights the systems requiring logical access controls based on data classification levels.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	An inventory of information assets, including hardware, software, processing facilities and data, is maintained and updated at least annually. All assets have an assigned asset owner. All assets are classified based on the data classification convention.	Inspected the Data Classification Policy to determine that the company assets are classified based on the data classification convention. Inspected Infrastructure documentation to determine that the company has an inventory of information assets (including hardware, software, and data), assets have an assigned asset owner and is updated at least annually.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from	Role based security is utilized to grant user access and to segregate access to sensitive data in production and supporting tools.	Inspected access review to determine that the company implements role-based security to grant user access and to segregate access to sensitive data in production and supporting tools.	No exceptions noted.

	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.	Unique usernames and passwords are required to authenticate all users. Exceptions are approved by the CEO.	Inspected user listings to determine that the company requires unique usernames and passwords to authenticate all users. Auditor noted no exceptions were approved during the audit period.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Authentication for the network, databases and applications adheres to the company password setting requirements.	Inspected password configuration settings to determine that Authentication for the network, databases and applications adheres to the company password setting requirements.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Administrator access to the application, database, network is restricted to authorized users.	Inspected access review to determine that the company's Administrator access to the application, database, network is restricted to authorized users.	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	Administrative and privileged access, as defined by policy, is reviewed at least annually.	Inspected the Logical Access Policy and Procedures to determine that the company's administrative and privileged access, as defined by policy, is reviewed at least annually.	No exceptions noted.

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	A user's access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket.	Inquired of company management and inspected the access reviews to determine that there were no terminations during the audit period.	Not tested. There were no terminations during the audit period.
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.	Management performs at least an annual review of user access to systems based on job duties. Inactive users are removed and removal is documented. The review is formally documented including system generated user listings and sign off by management.	Inspected access review to determine that the company's management performs at least an annual review of user access to systems based on job duties and the review is formally documented and signed off by management. Auditor noted no changes to the access review.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Developers do not have access to IT infrastructure tools or the production environment. Exceptions are documented and approved by the CEO.	Inspected users listings to determine that the developers do not have access to IT infrastructure tools or the production environment and exceptions are documented by the CEO.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Access to the source code repository is restricted to authorized employees.	Inspected the user listings to determine that access to the source code repository is restricted to authorized employees.	No exceptions noted.

CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Administrator access to the application, database, network is restricted to authorized users.	Inspected access review to determine that the company's Administrator access to the application, database, network is restricted to authorized users.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Segregation of duties exist during the infrastructure and application change process, enforced in the source control system (GitHub).	Inspected user listings to determine that the company implements segregation of duties during the infrastructure and application change process and is enforced in the source control system (GitHub).	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	A user's access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket.	Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	Not tested. There were no new hires during the audit period.
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.	Logical Access Policy and Procedures are in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege. The policy is reviewed annually.	Inspected the Logical Access Policy and Procedures, last reviewed during the audit period to determine that the company has Logical Access Policy and Procedures in place which define the authorization, modification, removal of access, role-based access, and the principle of least privilege and is reviewed annually.	No exceptions noted.
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	Administrative and privileged access, as defined by policy, is reviewed at least annually.	Inspected the Logical Access Policy and Procedures to determine that the company's administrative and	No exceptions noted.

	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.		privileged access, as defined by policy, is reviewed at least annually.	
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.	Data is disposed of according to the Data Retention, Disposal Policy and/or customer contract.	Inquired of company management to determine that there were no customer data deletion requests during the audit period.	Not tested. There were no customer data deletion requests during the audit period.
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.	Procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place.	Inspected the Data Retention Policy to determine that procedures are in place to remove data from production based on retention schedules, contract requirements, and deletion rules that are applied to specific forms of data; disposals are tracked; a data disposal process is in place.	No exceptions noted.
CC6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	A defined Data Management Policy provides guidance on information categories, usage, storage, and transmission of data.	Inspected the Data Management Policy and Procedures to determine that the company has defined the objectives and requirements for data retention and handling.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Firewall rulesets are configured and in place to help prevent unauthorized access threats from outside the application and infrastructure environment.	Inspected WAF ruleset to determine that firewall rulesets are configured and in place to help prevent unauthorized access threats from outside the application and infrastructure environment.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Production system access is encrypted to ensure communications with servers are secured.	Inspected the encryption in transit and server encryption to determine that production system access is encrypted to ensure communications with servers are secured.	No exceptions noted.
CC6.6	The entity implements logical access security	Threat detection tools are utilized to monitor and log	Inspected WAF configuration settings to determine that the company has a	No exceptions noted.

	measures to protect against threats from sources outside its system boundaries.	possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	threat detection tool in place that is utilized to monitor and log possible or actual network breaches and other anomalous security events and alerts occurring on threats and results are actioned as appropriate.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Remote access virtual private network sessions are encrypted.	Inspected the VPN encryption to determine that remote access virtual private network sessions are encrypted.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Disk encryption is enforced on all employee devices.	Inspected a sample of hard drive encryption settings to determine that the company disk encryption is enforced on all employee devices.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Any sensitive data that's transmitted over public networks, and data in transit is encrypted. HSTS compliance is maintained.	Inspected the encryption configurations to determine that sensitive data that's transmitted over public networks, and data in transit is encrypted, and HSTS compliance is maintained.	No exceptions noted.
CC6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	Remote access virtual private network sessions are encrypted.	Inspected the VPN encryption to determine that remote access virtual private network sessions are encrypted.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Vulnerability scans are performed annually to help identify security risks and results are triaged and actioned per Service Level Agreement.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no results were triaged and actioned per Service Level Agreement.	No exceptions noted.

CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Antivirus is installed on workstations and servers to help protect against viruses and malicious software on the systems.	Inspected a sample of antivirus configurations for workstations and servers to determine that antivirus is installed on workstations and servers to help protect against viruses and malicious software on the systems.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous security events. Alerting occurs on threats and results are actioned as appropriate.	Inspected WAF configuration settings to determine that the company has a threat detection tool in place that is utilized to monitor and log possible or actual network breaches and other anomalous security events and alerts occurring on threats and results are actioned as appropriate.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	A baseline security configuration is maintained and is deployed to all systems; the baseline settings are reviewed annually or as business needs change. This can be in the form of AWS deployment recipes.	Inspected Infrastructure documentation to determine that the company's baseline security configuration is maintained and is deployed to all systems; the baseline settings are reviewed annually or as business needs change.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Vulnerability scans are performed annually to help identify security risks and results are triaged and actioned per Service Level Agreement.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no results were triaged and actioned per Service Level Agreement.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An independent, third party provider is contracted to perform penetration tests at least annually. Test results are reviewed and tracked to resolution.	Inspected the penetration test report to determine that the company contracts an independent third-party provider to perform penetration tests at least annually and test results are reviewed and tracked to resolution.	No exceptions noted.
CC7.2	The entity monitors system components and the operation of those components for anomalies	Threat detection tools are utilized to monitor and log possible or actual network breaches and other anomalous	Inspected WAF configuration settings to determine that the company has a threat detection tool in place that is utilized to monitor and log possible or	No exceptions noted.

	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.	security events. Alerting occurs on threats and results are actioned as appropriate.	actual network breaches and other anomalous security events and alerts occurring on threats and results are actioned as appropriate.	
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	Vulnerability scans are performed annually to help identify security risks and results are triaged and actioned per Service Level Agreement.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least annually. Auditor noted that no results were triaged and actioned per Service Level Agreement.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	Inspected the Security Incident Response Policy and Plan and Incident Response template to determine that the company has an incident response process that includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	No exceptions noted.
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.	Inspected the Security Incident Response Policy and Plan to determine that the company has a documented incident response plan in place to guide employees in identifying, reporting, and acting on breaches and incidents. Inspected the Breach Template to determine that the company has a process in place to address data breaches.	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program	The incident response process includes a means to capture the data necessary to analyze an incident and determine the	Inspected the Security Incident Response Policy and Plan and Incident Response template to determine that the company has an incident response	No exceptions noted.

	to understand, contain, remediate, and communicate security incidents, as appropriate.	security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	process that includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	
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 design, implementation, maintenance, execution, and annual of the security incident response program and data breach response procedures are the responsibility of the CEO.	<p>Inspected the Information Security Policy and Disaster Recovery and Business Continuity Plan to determine that the security incident response program and data breach response procedures are the responsibility of the CEO.</p> <p>Inspected the tabletop exercise to determine that the company security incident response program and data breach response procedures are tested at least annually.</p>	No exceptions noted.
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.	<p>Inspected the Security Incident Response Policy and Plan to determine that the company has a documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents.</p> <p>Inspected the Breach Template to determine that the company has a process in place to address data breaches.</p>	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The incident response process includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	Inspected the Security Incident Response Policy and Plan and Incident Response template to determine that the company has an incident response process that includes a means to capture the data necessary to analyze an incident and determine the security impact, including documentation of: containment steps performed, mitigations, stakeholder notification, and steps to restore service. The organization performs a root cause analysis (RCA) for incidents and information disclosures that could impact security.	No exceptions noted.

CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Documented backup and restoration procedures for the network are maintained and reviewed annually.	Inspected the Data Backup and Restoration Policy, reviewed during the audit period to determine that the documented backup and restoration procedures for the network are maintained and reviewed annually.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A centralized ticketing and workflow tool tracks software change activity, including development, approvals and testing.	Inspected a sample of code changes to determine that the company has a A centralized ticketing and workflow tool that tracks software change activity, including development, approvals and testing.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Production, testing, and development environments are logically separated.	Inspected the separate production and staging environments to determine that production, testing, and development environments are segregated.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	A baseline security configuration is maintained and is deployed to all systems; the baseline settings are reviewed annually or as business needs change. This can be in the form of AWS deployment recipes.	Inspected Infrastructure documentation to determine that the company's baseline security configuration is maintained and is deployed to all systems; the baseline settings are reviewed annually or as business needs change.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	All application changes are developed, tested, reviewed, and approved prior to implementation.	Inspected a sample of code changes to determine that application changes are developed, tested, reviewed, and approved prior to implementation.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	An emergency change process is followed for changes required in urgent situations.	Inspected a sample of emergency code change deployments to determine that the company has an emergency change process for changes required in urgent situations.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or	A Change Management Policy and Procedures are in place to	Inspected the Change Management Policy to determine that the	No exceptions noted.

	acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	request, document, test, and approve changes.	company has documented the change process elements and controls.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	A Disaster Recovery Plan is maintained and tested annually.	Inspected the business continuity plan and annual business continuity test to determine that the company had maintained business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The organization clearly defines and documents vendor management roles, contract expectations, and vendor risks.	Inspected the Vendor Management Policy and vendor list to determine that the company clearly defines and documents vendor management roles, contract expectations and vendor risks.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Employees and contractors are required to sign a confidentiality policy upon hire. A non disclosure agreement is required for third parties that may have access to personal information. The non disclosure agreement includes the signee's and the company's responsibility with respect to information security. The template is periodically reviewed to align with business requirements.	Inspected confidentiality agreement to determine that the company periodically reviews the agreement to align with business requirements. Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A user's access to IT systems is revoked within 48 hours when employment or contract terminates. Exceptions are documented in the checklist and/or offboarding ticket.	Inquired of company management and inspected the access reviews to determine that there were no new hires during the audit period.	Not tested. There were no new hires during the audit period.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The organization utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers; scope, responsibilities, compliance requirements, and service levels are included in the contract.	Inspected the customer service agreement to determine that the company utilizes a standard contractual agreement that defines relevant security commitments and requirements for both its customers as well as third party providers.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	External parties may report system failures, incidents, concerns, and other complaints to appropriate personnel by	Inspected the contact page to confirm that external parties can report system failures, incidents, concerns, and other complaints by	No exceptions noted.

		submitting their issue via the organizations support webpage. The incident is documented in accordance with the Incident Response Plan, if required.	submitting their issues via the organization's support webpage. Inquired of company management to determine that there were no security incidents during the audit period.	Not tested. There were no security incidents during the audit period.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	A documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. A breach response plan/process is in place to address data breaches.	Inspected the Security Incident Response Policy and Plan to determine that the company has a documented incident response plan is in place to guide employees in identifying, reporting, and acting on breaches and incidents. Inspected the Breach Template to determine that the company has a process in place to address data breaches.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Third party SOC 2 reports are reviewed for impact to the organization's control environment, and the review is formally documented by management.	Inspected critical SOC 2 report and review to determine that the company maintains critical third-party SOC 2 reports and reviews are formally documented by management.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Due diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter. Due diligence activities include an assessment of information security practices based on the assessed level of vendor risk.	Inspected compliance reports, risk assessment, and reviews to determine that the company implements Due diligence activities are performed over new vendors prior to contract execution, and on an annual basis thereafter, this includes an assessment of information security practices based on the assessed level of vendor risk.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	An annual risk assessment is conducted to identify, assess, mitigate, report and monitor security, fraud, legal & regulatory, and vendor risks. Risks are scored by likelihood and impact, and high risks are actioned upon according to the risk assessment policy.	Inspected the risk assessment to determine that the company conducts an annual risk assessment to identify, assess, mitigate, report, and monitor security, fraud, legal and regulatory, and vendor risks.	No exceptions noted.