Simfoni USA Inc.

Report on Controls at a Service Organization Relevant to Security and Availability as of

December 31, 2020

SOC 2 Type 1

TABLE OF CONTENTS

SECTION I – INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor's Report

Mr. Jason Stern
Simfoni USA Inc.
549 W Randolph St Suite 700
Chicago, IL 60661

Scope

We have examined Simfoni USA Inc.'s ("Simfoni" or the "Company") accompanying description of its Spend Analytics Platform system found in Section III titled "Simfoni USA Inc.'s Description of its Spend Analytics Platform System" as of December 31, 2020 (the "description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report*, (the "description criteria") and the suitability of the design of controls stated in the description as of December 31, 2020, to provide reasonable assurance that the Company's service commitments and system requirements were achieved based on the trust services criteria relevant to Security and Availability (the "applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

Subservice Organization

The Company uses a subservice organization to provide data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company'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.

Complementary User Entity Controls

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

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

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

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Other Matters

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

Opinion

In our opinion, in all material respects—

a. the description presents the Company's Spend Analytics Platform system that was designed and implemented as of December 31, 2020 in accordance with the description criteria.
b. the controls stated in the description were suitably designed as of December 31, 2020 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary user entity controls assumed in the design of the Company's controls as of that date.

Restricted Use

This report is intended solely for the information and use of the Company; user entities of the Company's Spend Analytics Platform system as of December 31, 2020; business partners of the Company subject to risks arising from interactions with the Spend Analytics Platform system; practitioners providing services to such user entities and business partners; prospective user entities and business partners; and regulators who have sufficient knowledge and understanding of the following:

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

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Assure Professional, LLC
Clemson, South Carolina
January 15, 2021

SECTION II – ASSERTION OF SIMFONI USA INC.'S MANAGEMENT

SIMFONI

Assertion of Simfoni USA Inc.'s Management

We have prepared the accompanying description of Simfoni USA Inc.'s (the "Company") Spend Analytics Platform system titled "Simfoni USA Inc.'s Description of its Spend Analytics Platform System" as of December 31, 2020 (the "description") based on the criteria for a description of a service organization's system set forth in *DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (the "description criteria"). The description is intended to provide report users with information about the Spend Analytics Platform system that may be useful when assessing the risks arising from interactions with the Company's system, particularly information about system controls that the Company 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 and Availability (the "applicable trust services criteria") set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*.

The Company uses a subservice organization for data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the Company's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of the Company'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 the Company, to achieve the Company's service commitments and system requirements based on the applicable trust services criteria. The description presents the service organization's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of the service organization's controls.

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

1) The description presents the Company's Spend Analytics Platform system that was designed and implemented as of December 31, 2020 in accordance with the description criteria.
2) The controls stated in the description were suitably designed as of December 31, 2020 to provide reasonable assurance that the Company's service commitments and system requirements would be achieved based on the applicable trust services criteria, if the subservice organization and user entities applied the complementary controls assumed in the design of the Company's controls as of that date.

By: Jason Stern

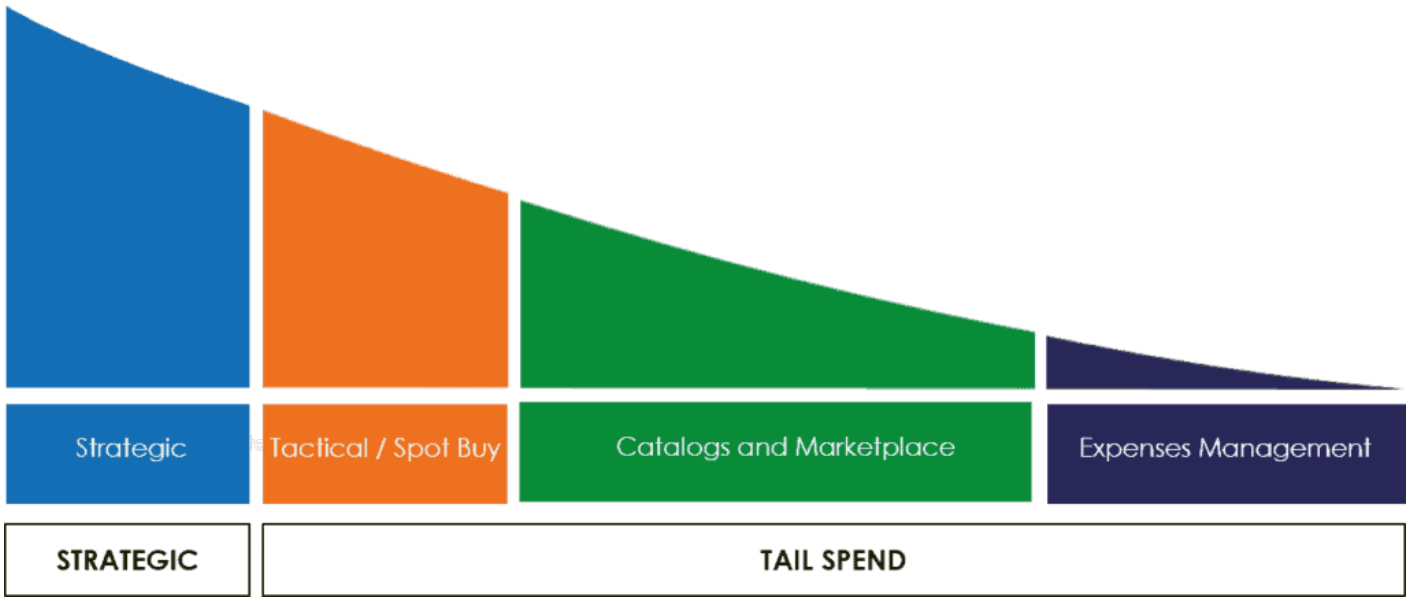
Title: CEO

January 15, 2021

SECTION III – SIMFONI USA INC.'S DESCRIPTION OF ITS SPEND ANALYTICS PLATFORM SYSTEM

Simfoni USA Inc.'s Overview & Services Provided

In 2015, Tail Spend was a largely ignored category due to challenges in managing it in a cost-effective manner. Simfoni recognized that this category was the last mile in sourcing and felt there was a better way. Bringing machine-learning driven automation and marketplace technology into this category represented a unique value proposition and an opportunity to help organizations manage their Tail Spend and control many suppliers.



However, to effectively manage this spend category as a service, Simfoni needed a Spend Analytics tool that could deliver an extremely granular classification with a quick implementation. Simfoni initially partnered with many analytics vendors but found that their legacy platforms lacked the capability to incorporate modern, AI-driven algorithms to generate the detailed visibility required. Also, they lacked the procurement expertise to understand how to generate insights to power the tail spend solution.

Instead, Simfoni decided to build a better 'mouse-trap' and Simfoni Analytics was born. By building the tool from scratch with Artificial Intelligence techniques at the core of the solution, Simfoni was able to solve the legacy issues of the traditional Spend Analytics products.

By 2018, Spend Analytics was being offered within the Spend Automation business and was extremely effective in identifying opportunities in the client's data and delivering value in both Tail Spend Management and eProcurement. However, Simfoni was so excited about the success of the Spend Analytics development that they decided to release the product to be sold directly to large enterprise customers who could use it to derive insights across their entire procurement spend, as well as other parameters such as supply risk, vendor diversity, and much more.

Today, Simfoni Analytics has been deployed globally by 100's of customers. It is licensed directly to both large global companies and leading procurement consultancies. Simfoni provides spend analytics and spend automation products to leading global enterprises. Their products provide rapid time to value through machine learning and artificial intelligence that accelerate and automate key aspects of the procurement process. Customers save both time and money, as well as identify strategies to reduce risk. A global business with regional headquarters in the USA, Europe, Australia and the Middle East, Simfoni works "in harmony" with its customers, their business stakeholders, and their vendor communities.

Boundaries of the Systems

The purpose of the system description is to delineate the boundaries of the system, which include the services outlined above and the five components described below: infrastructure, software, people, data, and procedures. The scope of this report includes the following Simfoni facilities that support the Spend Analytics Platform systems:

INFRASTRUCTURE

The Company's information system allows the Company to accept data from its clients using a variety of secure methods.

Facility	Service Provider	Function	Hosted Applications
Chicago, Illinois	N/A	Corporate Headquarters & Operations Center	N/A
N/A	AWS	Production & Development	Spend Analytics Platform

Note: Data hosting services are provided by a subservice organization ("Amazon Web Services (AWS)"). The data hosting environments are not included in the scope of this report.

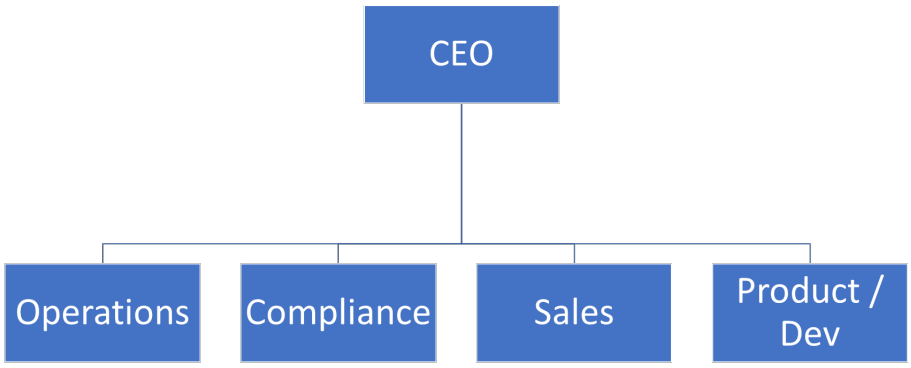
SOFTWARE

Software utilized by IT to manage and support the Environment includes:

- Backup management, (AWS)
- Anti-Virus, (ClamAV & McAfee)
- System & Network monitoring, (Elastic & AWS)
- Security monitoring, (*removed for security*)
- Change management, (GitLab & JIRA)

PEOPLE

The following functional areas / groups are used to support the services offered by the Company and are involved in governance, management, operation, security and use of the system.



Management Oversight and Organizational Structure

The Company's organizational structure provides the framework within which its activities for achieving entity-wide objectives are completed and analyzed. The Company is organized in a manner which defines key areas of authority while maintaining adequate separation of duties.

Roles and Responsibilities

Everyone at Simfoni has some responsibility for achieving the obligations of the Company. Proper lines of communication are in place to discuss operational activities and risks of the Company in a timely manner with management. The Company's management encourages individuals and teams to use initiative in addressing issues and resolving problems.

DATA

Data processed by the system is managed and stored in accordance with the relevant data protection policies and procedures. The data is managed, transmitted, and stored in a range of system and database technologies.

All data flowing through Simfoni infrastructure is restricted to authorized individuals requiring such access including the Company's customer base. Logical access controls ensure access is restricted to authorized individuals based on job functions.

PROCEDURES

Automated and manual procedures related to the services provided include procedures by which service activities are initiated, authorized, performed, and delivered and reports or other information is prepared.

Security is critical to the physical network, computer operating systems, and application programs. Each area offers its own set of security issues and risks. The Company has implemented a comprehensive security program that offers a high level of protection corresponding with the value of the assets.

Accountability

Individual users are responsible for ensuring that others do not access data or information from their systems. Users must take great care in protecting their usernames and passwords and this information is never to be loaned or given to other members of the Company or outside individuals. Disclosing this information could lead to vulnerabilities of the system as well as to the data and information contained on the system.

ADDITIONAL ELEMENTS OF THE CONTROL ENVIRONMENT

The Control Environment

The control environment sets the tone of an organization, influencing the control consciousness of its people. It is the foundation for all other components of internal control, providing discipline and structure. Control environment factors include the integrity and ethical values, competence of the entity's people; management's philosophy and operating style; the way management assigns authority and responsibility and organizes and develops its people; and the attention and direction provided by senior leadership. The Company has established controls which foster shared values and teamwork in pursuit of the organization's objectives.

Integrity and Ethical Values

Integrity and high ethical standards are qualities essential to the Company's business and are viewed as fundamental standards of behavior for all employees. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people, who create, administer, and monitor them. The Company established programs and policies designed to communicate and reinforce the integrity and ethical standards of the Company. Any employee found to have violated the ethics policy may be subject to disciplinary action, up to and including termination.

Commitment to Competence and Accountability

The Company defines competence as the knowledge and skills necessary to accomplish tasks that define an employee's roles and responsibilities. The Company seeks only high-quality staff with significant experience, education, and understanding of working in a team environment.

Human Resources Security

Simfoni observes Human Resources (HR) policies, procedures, and guidelines within its Employee Handbook. Management updates these policies as appropriate. Simfoni managers observe these policies, procedures, and guidelines as well as applicable federal and state laws, as they relate to recruitment, selection, and hiring of employees and contractors.

Management collects all company property and assets (e.g., company credit cards, keys, computer, cell phone, etc.) from terminated employees. All company proprietary files are secured, and access to all electronic resources (e.g., telephone, network, computer, email, etc.) is terminated.

Communications

The Company uses a variety of methods for communication to ensure that significant events and issues are sent in a timely manner and that staff understand their role and responsibility over service and controls. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

The Employee Handbook contains the principles that guide the conduct of employees and provides details of the personnel policies and benefits offered by Simfoni.

Policies

Simfoni maintains a suite of comprehensive policies designed to provide both management's stated direction (policy) and staff working practices (procedures). These documents are posted on the Company's intranet and are available to all employees.

Policies address the reasons for security; the rules and procedures required to achieve security; and the personnel and roles who work to enforce the security policies. The accompanying table lists an example of the policy documents that have been adopted by Simfoni.

Policies	Description
Acceptable Use Policy Security Awareness Bring Your Own Device (BYOD) Policy Employee Handbook	Policies governing how computing resources may be used.
Data Classification Policy Data Destruction Policy Confidentiality & Non-Disclosure Agreement	Policies related to the creation, exposure, and disposal of data, both corporate and client.
Information Security Policy User Right Assignment Reviews Password Policy	Policies that cover the security of network attached resources and the network infrastructure that serves these resources.
Backup Policy Disaster Recovery Plan Change Management Policy Incident Response	Policies, rules, and procedures covering actions that affect the ongoing maintenance and availability of a secure infrastructure.
Encryption Policy	Policies covering the security of Information Technology assets.

Published Job Descriptions

Job descriptions aid in establishing hiring criteria, orienting new employees to their jobs, identifying the requirements of each position, setting standards for employee performance evaluations, and establishing a basis for making reasonable accommodations for individuals with disabilities. Simfoni makes every effort to create and maintain accurate job descriptions for all positions within the organization. Each description at a minimum includes the job title and the duties for the position. Additional requirements are listed depending on the position.

Monitoring

Company management performs monitoring activities as part of normal business operations to assess the quality of the internal control environment. Management performs regular reviews of tasks assigned to their teams. Monitoring activities are used to initiate corrective action through team meetings, client conference calls, and informal notifications.

Performance Evaluations

Simfoni employees undergo performance reviews to identify both strengths and areas in need of improvement. All employees, regardless of classification or length of service, are expected to meet and maintain company standards for job performance and behavior.

Support Operations

Simfoni maintains systems that manage the flow of information and facilitate communications with its customers. Customers report issues with the services provided either through a phone call or email to customer support. These items are ticketed and tracked for timely resolution.

Risk Assessment

Every entity faces a variety of risks from external and internal sources that must be assessed. A precondition to risk assessment is establishment of objectives, linked at different levels and internally consistent. Risk assessment is the identification and analysis of relevant risks to the achievement of Company objectives and forming a basis for determining how the risks should be managed. Because economic, industry, regulatory and operating conditions will continue to change, mechanisms are needed to identify and deal with the special risks associated with change.

Management identifies risks that threaten client commitments by performing a formal risk assessment annually. The risk assessment includes the analysis of fraud, threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Management holds risk management meetings throughout the year so that it can react swiftly to address emerging risks. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference of risk through insurance policies.

The Company maintains insurance coverage to transfer certain identified risks. The company maintains a general liability and umbrella policy to protect against unforeseen events. Additional insurance policies may be acquired as needed to satisfy certain contractual obligations.

Control Activities

Security Management

Simfoni implements Security practices to help protect access to data and systems and to limit access to authorized personnel. Simfoni has instituted Security Awareness Training and the Simfoni workforce is trained on security expectations.

Additionally, Simfoni meets periodically to discuss current security issues and concerns for its services.

<u>Information Security</u>

The information security program provides reasonable protection against unauthorized access, disclosure, modification, or destruction, as well as to assure the availability, usability, and authenticity of information. This applies to all systems that manage or store data.

<u>Logical Access</u>

Access to resources and data are granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests.

Individual access capabilities are removed immediately by IT or data owners upon the notification of termination of employment, change of responsibilities, or termination of a contract with a client that uses the system. System security access levels are periodically reviewed by IT and data owners to ensure individual access rights are appropriate based on job information.

Password Settings
Simfoni follows structured user and password management procedures. Simfoni utilizes an initial strong complex password for the user. All user accounts password is set to expire after a set number of days. Password history, maximum password age, minimum password age and minimum password lengths are enabled and established.

Computer Operations & Data Communications

The Company utilizes several network security technologies to protect and defend Internet-accessible systems.

Firewalls
Firewalls protecting the intranet from the public network are implemented, configured, and managed by the Simfoni administration staff. Firewalls utilized access rules to grant or deny access to internal resources.

Data Transmission and Encryption
Data in motion is encrypted using SSL level encryption.

Incident Response

Incident management is not only a necessary practice for internal Simfoni operations, but it is also a key component fulfilling Simfoni's obligations to its Customers regarding the service offerings. Effective incident management can ensure Simfoni operations, reduce downtime, and increase customer confidence in Simfoni's ability to service its outsourcing needs.

Backup and Disaster Recovery

Simfoni has implemented various backup methods as part of its production operations. Automated software is utilized to perform the backups of production servers. System snapshots are taken to restore systems in accordance with established recovery point objectives.

Backup Testing
Restores from backups are performed as an ongoing component of normal business operations. Servers can be restored from backup snapshots to deploy new server instances or for development and testing purposes.

Recovery
Simfoni has a documented recovery plan in place. Periodically, the plan is tested through a series of exercises from tabletop to complete restore events. Any issues resulting from these tests are incorporated into the plan and updates are made accordingly.

Network Monitoring

Monitoring policies and procedures are utilized for addressing issues relating to outages of critical services or other issues needing immediate action. These procedures vary based on the defined severity level of the problem. Company engineers use several monitoring tools to identify and provide alerts.

Simfoni utilizes a suite of monitoring tools to provide proactive incident identification and response services. The Company's Information Technology team regularly monitors the network. Overall health and capacity planning are monitored to ensure the system will meet clients' needs. The monitoring applications generate alerts when predefined thresholds are exceeded on the monitored devices. Information Technology monitors security access violations, including server logs and reports.

System Maintenance and Change Management

Software Development Life Cycle ("SDLC")
Simfoni follows a controlled approach to developing, testing, approving, and building each release of the system that is designed to ensure continued quality of the released product before it is available to the client base.

A software application is used to manage the application development tickets utilizing a defined process. The Development Team utilizes defined code review and a code checklist in the development of applications. Versioning control software is also used to maintain current and historical versions of files such as source code, web pages, and documentation.

Simfoni maintains segregated access and permissions to the different environments. Only properly tested and properly authorized changes to the production environment are deployed.

Complementary Controls at User Organizations

The Company's applications are designed with the assumption that certain controls would be implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report.

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether the following controls have been placed in operation at the user organizations:

Security (Common Criteria)

ID	Criteria
CC 2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
	• User organizations are responsible for controls to input complete and accurate information and comply with the operating instructions of the Company's products and applications.
CC 2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
	• User organizations are responsible for controls to comply with the operating instructions of the Company's products and applications.
CC 2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.
	• User organizations are responsible for controls to communicate with the company regarding failures, incidents, concerns, and other matters when complying with the operating instructions of the Company's products and applications.

Security (Common Criteria, Continued)

ID	Criteria (Continued)
CC 3.2	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.
	• User organizations are responsible for informing the Company of any regulatory issues that may affect the services provided by the Company.
CC 3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
	• User organizations are responsible for risks related to the use of IT and access to information when granting access to the services provided by the Company.
CC 3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.
	• User organizations are responsible for controls to comply with the operating instructions of the Company's products and applications. • User organizations are responsible for controls to notify the Company in a timely manner when changes are made to technical, billing, or administrative contact information.
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.
	• User organizations are responsible for controls to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis. • User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users, whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
	• User organizations are responsible for controls to ensure that user organizations adopt strong operating system and application password management procedures, including using passwords that cannot be easily compromised and require to change on a regular basis. • User organizations are responsible for controls to ensure the confidentiality of any user IDs and passwords assigned.

ID	Criteria (Continued)
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	• User organizations are responsible for controls to notify the Company in a timely manner when changes are made to technical, billing, or administrative contact information.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
	• User organizations are responsible for procedures to define developing, maintaining, and testing their own business continuity plans ("BCP").
CC 6.7	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.
	• User organizations are responsible for controls to provide reasonable assurance of the transmission and receipt of information not provided by the Company.
CC 7.2	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.
	• User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.
CC 7.3	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.
	• User organizations are responsible for controls to immediately notify the Company of any actual or suspected information security breaches, including compromised user accounts.

Availability

ID	Criteria
A 1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	• User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans ("BCP"). • User organizations are responsible for approving the telecommunications infrastructure controls between itself and the Company.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
	• User organizations are responsible for controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans ("BCP").

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Processing of information for customers by the Company covers only a portion of the overall internal control structure of each customer. The Company's products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all the control objectives relating to the processing of transactions to be completely achieved by the Company. Therefore, each customer's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Subservice organization controls related to the Trust Services Principles

Infrastructure – All networking, servers, backup and disaster and recovery infrastructure, connection points, routing equipment, firewalls, and internet service provider connections required in the hosted production environment is maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit report on the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Software – Applications required for the hosted production environment including network operating systems, virtual services, application and performance monitoring, malicious code management, intruder detection and prevention, data backup and replication including disaster recovery required in the hosted production environment is maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

People – Personnel required for the maintenance and operation of the hosted production environment is maintained by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Procedures - All procedures required to meet the Service Level Agreements (SLA) in the operation of the hosted production environment is maintained by the service organization. Physical access controls and procedures as well as environmental controls and procedures are provided by the subservice organization.

Controls in operation are verified annually by the service organization through the review of the independent third-party audit of the subservice organization controls and operating effectiveness (SOC 2 Type 2).

Data – Subservice organizations do not process data for the service organization and its users.

The following are applicable trust service criteria that are intended to be met by controls at the subservice organization and the types of controls expected to be implemented at the subservice organization that are necessary to meet the criteria, alone or in combination with controls at Simfoni USA Inc.

Security Principle – Criteria expected to be addressed by the subservice organization

ID	Common Criteria
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC 6.5	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.
CC 7.3	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.
CC 8.1	The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Availability Principle – Criteria expected to be addressed by the subservice organization

ID	Criteria
A 1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
A 1.2	The entity authorizes, designs, develops, or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
A 1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.

Trust Services Criteria Not Relevant to the System

ID	Criteria	Reason for Exclusion
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	Simfoni does not have an *independent* Board of Directors.
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	Production infrastructure and its security is the responsibility of subservice organizations.

Significant Changes to the System

No significant events or conditions were noted by management during the audit examination period.

Trust Services Categories and Related Control Activities

The Trust Services Categories and related control activities are included in Section IV of this report and have been removed from the description to eliminate redundancy. The control activities listed in Section IV are, nevertheless, an integral part of the Company's description of controls.

The description of the service auditor's tests of operating effectiveness and the results of those tests are also presented in Section IV, adjacent to the service organization's description of controls. The description of the tests of operating effectiveness and the results of those tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS

Trust Services Principle – Common Criteria
Common Criteria to Security and Availability

CC1.0	Common Criteria Related to Control Environment
TSP	**Description of Controls in Place**
CC1.1	The entity demonstrates a commitment to integrity and ethical values as they relate to Security and Availability.
	• The Company has a code of conduct that guides employees on the Company's principles and conduct. • Employee evaluations are performed on a regular basis against individual objectives derived from the Company's goals, established standards, and specific job responsibilities. • There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives as they relate to Security and Availability.
	• Organizational charts are in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. • The Company is segregated into separate and distinct functional areas for the purposes of the management and processing of customer information. • The Company has documented job descriptions that describe the roles and responsibilities of the position.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives as they relate to Security and Availability.
	• The Company has an employee handbook that describes management's philosophy, operating style, and provides HR policy guidance to employees. • Management has documented its human resource policies and practices. • During the hiring process, a reference check is performed on potential employees before they begin employment with the Company. • Employee evaluations are performed on a regular basis against individual objectives derived from the Company's goals, established standards, and specific job responsibilities. • Staff are given Security Awareness training during their new hire onboarding and are then updated on an annual basis.

CC1.0	Common Criteria Related to Control Environment (Continued)
TSP	**Description of Controls in Place**
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives as they relate to Security and Availability.
	• The Company has an employee handbook that describes management's philosophy, operating style, and provides HR policy guidance to employees. • Employee evaluations are performed on a regular basis against individual objectives derived from the Company's goals, established standards, and specific job responsibilities. • There is a formal discipline policy for employees who are suspected of rule infractions or violations of company policies. • An Acceptable Use Policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.

CC2.0	Common Criteria Related to Communication and Information
TSP	**Description of Controls in Place**
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control as they relate to Security and Availability.
	• The Information and Application Security Policies are reviewed annually, updated, and approved by management to remain current. • A monitoring application is utilized to monitor network devices and critical systems. • Status reports from the enterprise monitoring applications can be generated for adhoc review. • The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • Security event logging is configured to log specific events on the network domain. • A third-party application is used to monitor network devices and to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control as they relate to Security and Availability.
	• The Company has documented job descriptions that describe the roles and responsibilities of the position. • Security Planning and Maintenance responsibilities have been delegated. • A description of the system is posted on the entity's shared drive and is available to the entity's internal users. This description delineates the boundaries of the system and key aspects of processing. • The Company publishes its information security policies and organizational procedures on its corporate shared drive. • Staff are given Security Awareness training during their new hire onboarding and are then updated on an annual basis.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control as they relate to Security and Availability.
	• A description of the system is posted on the Company's Public Web Site and is available to users. • Management has documented support operations procedures to outline how customer reported issues are addressed and resolved. • Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.

CC3.0	Common Criteria Related to Risk Assessment
TSP	**Description of Controls in Place**
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives as they relate to Security and Availability.
	• Management meetings are held on a regular basis to discuss operational issues. • The Company has a risk management program to address security and business-related risks. • Risk Committee meetings are held quarterly to monitor the controls of the company.
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 as they relate to Security and Availability.
	• Risk Committee meetings are held quarterly to monitor the controls of the company. • The Company completes a risk assessment and updates the list of identified risks periodically. • The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.

CC3.0	Common Criteria Related to Risk Assessment (Continued)
TSP	**Description of Controls in Place**
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives as they relate to Security and Availability.
	• The Company has a risk management program to address security and business-related risks. • Risk Committee meetings are held quarterly to monitor the controls of the company. • The Company completes a risk assessment and updates the list of identified risks periodically.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control as they relate to Security and Availability.
	• The Company's application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC. • Source code management software is utilized for version control of development projects and to control access to source code libraries. • A tracking system is used to log critical and non-critical application change requests (issues/projects) reported by users or internal parties. • An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems. • Changes to the production environment are documented in the ticketing system and a work order is created. • Management has documented support operations procedures to outline how customer reported issues are addressed and resolved. • Customer reported problems are entered into a trouble ticket system. Tickets are opened, investigated, and resolved per problem management procedures.

CC4.0	Common Criteria Related to Monitoring Activities
TSP	**Description of Controls in Place**
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 as they relate to Security and Availability.
	• Management meetings are held on a regular basis to discuss operational issues. • Employee evaluations are performed on a regular basis against individual objectives derived from the Company's goals, established standards, and specific job responsibilities.
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, as they relate to Security and Availability.
	• The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.

CC5.0	Common Criteria Related to Control Activities
TSP	**Description of Controls in Place**
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels as they relate to Security and Availability.
	• A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks. • A redundant firewall is in place and has been configured as a fail-over to the primary firewall. • Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel. • An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives as they relate to Security and Availability.
	• The Company has a risk management program to address security and business-related risks. • Security Planning and Maintenance responsibilities have been delegated. • A monitoring application is utilized to monitor network devices and critical systems. • A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices. • Antivirus software scans production servers and workstations on a real-time basis. • Antivirus software is configured to automatically update servers and personal computers on a daily basis.

CC5.0	Common Criteria Related to Control Activities (Continued)
TSP	**Description of Controls in Place**
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action as they relate to Security and Availability.
	• The Company has an Information Security Policy that describes the security posture and practices of the Company. • The Information and Application Security Policies are reviewed annually, updated, and approved by management to remain current. • The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards. • Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information. • Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations. • The Company's application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC. • An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems. • Management has documented support operations procedures to outline how customer reported issues are addressed and resolved.

CC6.0	Common Criteria Related to Logical and Physical Access Controls
TSP	**Description of Controls in Place**
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 as they relate to Security and Availability.
	• New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities. • Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards. • Passwords must conform to minimum requirements as enforced by the application. Password complexity standards are established to enforce control over access control software passwords. • Corporate domain administrator rights are restricted to specific network operations personnel. • Security groups have been configured and are enforced by the production network and servers to ensure access is restricted to sensitive data stored on the network. • Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities. • Management maintains a data encryption policy and procedure that provides guidance on Company standards for sending and receiving sensitive information. • A clear desk policy for papers and removable storage media is in place.
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.
	• New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities. • Management utilizes and retains termination checklists as confirmation of the revocation of system and facility access privileges as a component of the employee termination process. • Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities. • Termination procedures are in place for the removal of access to all systems upon notification of the termination.

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)
TSP	**Description of Controls in Place**
CC6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.
	• New hire checklists are used to ensure new staff receive the appropriate level of access to information systems and facilities. • Management utilizes and retains termination checklists as confirmation of the revocation of system and facility access privileges as a component of the employee termination process. • Security groups have been configured and are enforced by the production network and servers to ensure access is restricted to sensitive data stored on the network. • Monitoring audits of all user account rights assignments are performed periodically to ensure staff have the correct level of access to target systems for their job responsibilities. • Termination procedures are in place for the removal of access to all systems upon notification of the termination.
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 as they relate to Security and Availability.
	• Policies and procedures are in place to guide personnel on their responsibility for the classification of data and documents. • Policies and procedures are in place to guide personnel on their responsibility for the retention of data and documents. • Documented procedures are in place for rendering all sensitive information unreadable before being discarded or recycled.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries as they relate to Security and Availability.
	• Management maintains documented account management policies and procedures to provide guidance on the management of user accounts on target systems and password standards. • A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks. • Secure communication tunnels are in place for file transfers requiring encryption to the company's servers through the use of SSL encryption.

CC6.0	Common Criteria Related to Logical and Physical Access Controls (Continued)
TSP	**Description of Controls in Place**
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 as they relate to Security and Availability.
	• The Company has a Bring Your Own Device / Mobile Device policy to establish governance on the use of personal non-company owned digital devices accessing the Company infrastructure and its resources requiring standards for encryption and data protection of the device. • Corporate domain administrator rights are restricted to specific network operations personnel. • Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel. • Secure communication tunnels are in place for file transfers requiring encryption to the company's servers through the use of SSL encryption. • Management requires disk level encryption for laptops.
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 as they relate to Security and Availability.
	• Antivirus software is configured to automatically update servers and personal computers on a daily basis. • A third-party application is used to monitor network devices and to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives. • An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.

CC7.0	Common Criteria Related to System Operations
TSP	**Description of Controls in Place**
CC7.1	To meet its objectives, as they relate to Security and Availability, 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 monitoring application is utilized to monitor network devices and critical systems. • A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices. • A third-party application is used to monitor network devices and to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives. • Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.
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 as they relate to Security and Availability.
	• The Company has a risk management program to address security and business-related risks. • A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices. • Status reports from the enterprise monitoring applications can be generated for adhoc review. • The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • Security event logging is configured to log specific events on the network domain. • A third-party application is used to monitor network devices and to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives. • An Intrusion Prevention Systems (IPS) is utilized to continuously monitor the network for malicious activity and unauthorized access attempts.

CC7.0	Common Criteria Related to System Operations (Continued)
TSP	**Description of Controls in Place**
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 as they relate to Security and Availability.
	• The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • The Incident Response Procedures require that all security events (actual or suspected) be reported to appropriate management personnel. • The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response form is created as evidence of the assessment. • The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a review is to be conducted at the end of the process to identify any required changes to documented procedures. • The Incident Response Procedures documents the required procedures for evidence collection. • A third-party application is used to monitor network devices and to identify trends that may have a potential impact on the entity's ability to achieve its system security objectives.
CC7.4	The entity responds to identified security incidents, as they relate to Security and Availability, by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
	• The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • The Incident Response Procedures require that all security events (actual or suspected) be reported to appropriate management personnel. • The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response form is created as evidence of the assessment. • The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a review is to be conducted at the end of the process to identify any required changes to documented procedures. • The Incident Response Procedures documents the required procedures for evidence collection.

CC7.0	Common Criteria Related to System Operations (Continued)
TSP	**Description of Controls in Place**
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents as they relate to Security and Availability.
	• Management maintains documented backup schedules, policies, and procedures. • Restores from backups are performed to verify that system components can be recovered from backup media. • The Company has Security Incident Response Policy and Procedures in place to provide policy guidance and establish responsibilities for responding to and reporting security breaches. • The Incident Response Procedures require that all security events (actual or suspected) be assessed and classified, a documented response form is created as evidence of the assessment. • Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations. • Certain aspects of the disaster recovery plan are tested on an annual basis.

CC8.0	Common Criteria Related to Change Management
TSP	**Description of Controls in Place**
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 as they relate to Security and Availability.
	• An Infrastructure Change Management Policy is in place to guide personnel on documenting and implementing change control procedures that affect production systems. • The Company's application program code is designed and documented in accordance with written standards and procedures established by management in the SDLC. • A tracking system is used to log critical and non-critical application change requests (issues/projects) reported by users or internal parties. • Separate source code environments exist for development and production to prevent making changes that would affect the performance, and availability of production application code. • QA testing is documented and performed for development and maintenance activities prior to production release. • Development projects are reviewed and approved by management prior to implementation into the production environment. • Management restricts the ability to move code into the production environment to specific personnel. • Changes to the production environment are documented in the ticketing system and a work order is created.

CC9.0	Common Criteria Related to Risk Mitigation
TSP	**Description of Controls in Place**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions as they relate to Security and Availability.
	• The Company maintains insurance policies to mitigate losses and transfer certain identified risks. • The Company has a risk management program to address security and business-related risks. • The Company conducts an annual vendor assessment and evaluates and reviews independent 3rd party assessments on contracted subservice organizations and vendors. • The Company completes a risk assessment and updates the list of identified risks periodically. • Vulnerability assessments are performed by a third-party vendor periodically to test for known vulnerabilities on the network and production systems.
CC9.2	The entity assesses and manages risks associated with vendors and business partners as they relate to Security and Availability.
	• A Policy is in place to review and monitor the ongoing performance of the sub-service organizations. • The entity assesses the risks that vendors and business partners will fail to meet the entity's requirements.

Trust Services Principle – Availability
The system is available to users as committed or agreed

A1.0	Additional Criteria Related to Availability
TSP	**Description of Controls in Place**
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.
	• A monitoring application is utilized to monitor network devices and critical systems. • A monitoring application sends e-mail alert notifications to operations personnel when predefined thresholds are exceeded on monitored network devices. • The use of the system components is measured to establish a baseline for capacity management and to use when evaluating the risk of impaired availability due to capacity constraints.
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.
	• Management maintains documented backup schedules, policies, and procedures. • Automated backup systems are utilized to perform the scheduled system backups of target data. • Backup jobs are monitored, and notification alerts are sent in the event of backup failure. • The Company utilizes an internet backup system to backup certain servers and critical data to a secure, remote location. • Restores from backups are performed to verify that system components can be recovered from backup media. • The Company utilizes an internet backup system to backup certain servers and critical data to a secure, remote location.
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.
	• Restores from backups are performed to verify that system components can be recovered from backup media. • The Company utilizes an internet backup system to backup certain servers and critical data to a secure, remote location. • Certain aspects of the disaster recovery plan are tested on an annual basis.