SourceOne
OUTPUT TECHNOLOGIES
A Division of SourceOne Graphics, Inc.

SourceOne Output Technologies, Inc.

SOC 2 Type 2

Independent Service Auditor's Report on Management's Description of a Service Organization's System and the Suitability of the Design and Operating Effectiveness of Controls Relevant to Security and Availability

March 1, 2021 – February 28, 2022

ASCEND
AUDIT & ADVISORY

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701

TABLE OF CONTENTS

I. Independent Service Auditor’s Report

200 Second Avenue South, Suite 478
St. Petersburg, FL 33701
www.ascendaudit.com

Independent Service Auditor's Report

The Management of SourceOne Output Technologies, Inc.
711 Bond Avenue
Little Rock, AR 72202

Scope

We have examined SourceOne Output Technologies, Inc.'s ("SourceOne", or "the Company") description of controls for its marketing, print, and fulfillment system and related transactions throughout the period March 1, 2021 through February 28, 2022, based on the criteria for a description of a service organization's system in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, Description Criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period March 1, 2021 through February 28, 2022, to provide reasonable assurance that SourceOne's service commitments and system requirements were achieved based on the trust service criteria for security and availability set forth in DC section 200, *2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, Technical Practice Aids).

Subservice Organizations

SourceOne utilizes an enterprise grade FTP platform which is hosted in a third party data center. The description of the system in Section II of this report includes only the control objectives and related controls of the Company and excludes the control objectives and related controls at the subservice organization. Our examination did not extend to controls at the subservice organization.

SourceOne Output Technologies, Inc.'s Responsibilities

SourceOne 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 SourceOne's service commitments and system requirements were achieved. In Section II, SourceOne has provided its assertion titled "Assertion of SourceOne Output Technologies, Inc. Service Organization Management" about the description and the suitability of design and operating effectiveness of controls stated therein. SourceOne 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.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the description on the suitability of the 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 American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments as 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 users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of 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 and 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 policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of our tests are presented in Section III of our report.

Opinion

In our opinion, in all material respects,

a. the description presents the SourceOne system that was designed and implemented throughout the period March 1, 2021 through February 28, 2022, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period March 1, 2021 through February 28, 2022 and designed to provide reasonable assurance that SourceOne's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. the controls stated in the description operated effectively throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance that SourceOne's service commitments and system requirements were achieved based on the applicable trust services criteria.

Restricted Use

This report and the description of tests of controls and results thereof in Section III, is intended solely for the information and use of the Company, user entities of the Company's system throughout the period March 1, 2021 through February 28, 2022, and prospective user entities, independent auditors, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the Company
- How the Company's system interacts with user entities, subservice organizations, or other parties
- Internal control and its limitations
- Complementary user-entity controls and how they interact with related controls at the Company to meet the applicable trust services criteria
- The applicable trust services criteria
- The risks that may threaten the achievement of the applicable trust services criteria 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.

Ascend Audit & Advisory

ASCEND
AUDIT & ADVISORY

March 26, 2022

II. Information Provided by SourceOne Output Technologies, Inc.

ASSERTION OF SOURCEONE OUTPUT TECHNOLOGIES, INC. SERVICE ORGANIZATION MANAGEMENT

We have prepared the description of SourceOne Output Technologies, Inc.'s marketing, print, and fulfillment system ("system" or "the system") throughout the period March 1, 2021 through February 28, 2022, ("the description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization System in a SOC 2 Report* (AICPA, Description Criteria). The description is intended to provide report users with information about the system that may be useful when assessing the risks arising from interactions with SourceOne Service Organization's system, particular information about system controls that SourceOne 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 set forth in DC section 200, *2018 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA Trust Services Criteria).

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

a. The description presents the SourceOne system that was designed and implemented throughout the period of March 1, 2021 through February 28, 2022, in accordance with the description criteria.

   i. The description contains the following information:

      (1) The types of services provided.

      (2) The components of the system used to provide the services, which are the following:

      - *Infrastructure* – The physical and hardware components of a system (facilities, equipment, and networks).
      - *Software* – The programs and operating software of a system (systems, applications, and utilities).
      - *People* – The personnel involved in the operation and use of a system (developers, operators, users, and managers).
      - *Procedures* – The automated and manual procedures involved in the operation of a system.
      - *Data* – The information used and supported by a system (transaction streams, files, databases, and tables).

      (3) The boundaries or aspects of the system covered by the description.

      (4) How the system captures and addresses significant events and conditions.

      (5) The process used to prepare and deliver reports and other information to user entities and other parties.

      (6) If information is provided to, or received from, subservice organizations or other parties, how such information is provided or received; the role of the subservice organization and other parties; and the procedures performed to determine that such information and its processing, maintenance, and storage are subject to appropriate controls.

(7) For each category being reported on, the applicable trust services criteria and the related controls designed to meet those criteria, including, as applicable, complementary user-entity controls contemplated in the design of the Company's system.

(8) For subservice organizations presented using the carve-out method, the nature of the services provided by the subservice organization; each of the applicable trust services criteria that are intended to be met by controls at the subservice organization, alone or in combination with controls at the Company, and the types of controls expected to be implemented at carved-out subservice organizations to meet those criteria; and for privacy, the types of activities that the subservice organization would need to perform to comply with privacy commitments.

(9) Any applicable trust services criteria that are not addressed by a control at the Company or a subservice organization and the reasons, therefore.

(10) Other aspects of the Company's control environment, risk assessment process, information and communication systems, and monitoring of controls that are relevant to the services provided and the applicable trust services criteria.

(11) Relevant details of changes to the Company's system during the period covered by the description.

ii. The description does not omit or distort information relevant to the Company's system while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to his or her own particular needs.

b. The controls stated in the description were suitably designed throughout the period March 1, 2021 through February 28, 2022, to provide reasonable assurance that SourceOne's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period.

c. The controls stated in the description operated effectively throughout the period March 1, 2021 through February 28, 2022, to provide reasonable assurance that SourceOne's service commitments and system requirements were achieved based on the applicable trust services criteria.

By: /S/ Scott Caldarera

Scott Caldarera
Chief Information Officer

March 26, 2022

Description of SourceOne Output Technologies, Inc.'s Marketing, Print, and Fulfillment System

Company Overview

SourceOne Graphics, Inc. was founded in 1993. President and CEO Chris Cronin began SourceOne to fill a need in the market for an end-to-end production management company. His vision forged a company focused on project management from inception to delivery. SourceOne insures the quality and project oversight by helping customers develop new projects, including the integration of collateral from multiple vendors and markets. Working within tight time frames drove SourceOne to integrate key parts of the delivery cycle, in-house, as slow external processes were not keeping pace with rapidly decreasing turnaround times.

In 2008, SourceOne Graphics, Inc. completed a rebranding. The rebranding as SourceOne Output Technologies more clearly defines SourceOne as a print to mail and electronic file delivery company. While still maintaining all capabilities and expertise, data processing and intelligent inserting capabilities had grown exponentially, with a strong focus on secure document processing.

Committed to direct mail marketing since 1948, LSC (formerly Lloyd Schuh Company) was incorporated into SourceOne in 2014. With the latest mailing technology and the same reliable staff, LSC is known for keeping postal distribution options affordable and reliable even as mailing costs waver.

Services Overview

SourceOne's Wheeler Printing operation provides printing services with the ability to produce anything from a business card to a multi-page book with its four and two color press.

SourceOne also provides data documenting services, monochrome printing services, high speed ink printing, folding, inserting, and mailing services.

System Description

Services Provided

SourceOne provides mailing list management, printing and direct mailing services to the insurance, financial, government, third party administrators, small to large business, non-profit, advertising agencies, and political sectors.

Principal Service Commitments and System Requirements

SourceOne's principal service commitments, as they relate to the system description and the applicable trust services categories of security and availability are:

- Data – updating and maintaining client lists using advanced database technology and services;
- Mailing – by using advanced software and other postage reduction technologies; and
- Printing – using client data to print and assemble documents on-demand.

SourceOne's principal system requirements, as they relate to the system description and the applicable trust services categories of security and availability, are to provide:

- High-security statements, invoices, tax forms, and other transactional document generation
- Data validation and standardization
- Postage reduction technologies
- Business interruption protection
- Selectable and variable inserting
- Intelligent barcode-driven printing and processing
- Print production, procurement, and management
- Print material storage and distribution

Components of the System

This SOC 2 examination covers the SourceOne Infrastructure Environment ("IT Environment" or "System") including: operations, database administration, storage management, server administration, change management, system backup, and disaster recovery processes, as well as network operations, system monitoring tools and processes, system security (both logical and physical), and common support processes, applicable to all lines of business.

The System is comprised of the following components:

- Infrastructure (facilities, equipment, and networks)
- Software (systems, applications, and utilities)
- People (developers, operators, users, and managers)
- Procedures (automated and manual)
- Data (transaction streams, files, databases, and tables)

The following sections of this description define each of these five components comprising the System.

I*nfrastructure*

The SourceOne (IT) environment includes one data center, located in Little Rock, Arkansas, in the United States. Housed within this data center is the supporting operating system platforms (Windows based), networking components (routers, switches, firewalls), and data storage devices. The IT personnel that support this data center are based at the Company's corporate office facilities in Little Rock, Arkansas. All points of access to the corporate office are monitored by video cameras, including the external grounds.

Infrastructure Services is responsible for supporting multiple servers for in-scope technology solutions. These servers are summarized below by operating system and various purposes served.

Operating System	Server Purpose
Windows Server 2012	Monitoring Tools Application File Sharing Database Backup Domain CRM

Software

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

- Back up management
- System monitoring
- Job scheduling, processing, and monitoring
- Network monitoring
- Security monitoring
- Change management

People

IT personnel provide the following core support services over the SourceOne IT Environment components:

- Systems and Network Monitoring
- Security
- Database Administration
- Backup Operations
- Network Management
- Application Change Management
- Infrastructure Change Management

In order to provide these services, IT is divided into two functional areas: Network Management Services and Data Services. Below is a brief description of each of these functional areas:

- <u>Network Management Services:</u> The team deals with Fault, Configuration, Accounting, Performance and Security (FCAPS) - It keeps the network up and running smoothly, and monitors the network to spot problems as soon as possible, ideally before users are affected, keeping track of resources on the network and how they are assigned.
- <u>Data Services:</u> The team takes client or third party supplied data and processes to meet USPS mailing standards.

Procedures

SourceOne has documented policies and procedures to support the operations and controls over its IT Environment.

Specific examples of the relevant policies and procedures include the following:

- Policy management and communication
- System security administration
- Server security configuration
- Computer operations
- Network operations
- Disaster recovery planning
- Change management
- Incident/Problem management
- Physical security
- Backup and secured storage

Data

Infrastructure Services manages all database platforms within the IT Environment. Access to data is limited to authorized personnel in accordance with the Company's system security administration policies.

IT is responsible for the overall availability of data, including system backups, monitoring of data processing and file transmissions, as well as identifying and resolving problems.

Disclosures

System Incidents

For the period under review, there were no reported incidents originated from SourceOne. There were no material changes committed during the period that were within the boundaries of the System Description.

Criteria Not Applicable

Informed by Management the entity did not develop, manage, or maintain software and related software development activities. Software development was not applicable for the period under review.

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, and Information and Communication

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. The control environment has a pervasive influence on the structure of business activities, establishment of objectives, and assessment of risks. It influences control activities, information and communication systems, and monitoring procedures. The control environment is influenced by an entity's history and managerial culture. Effectively controlled entities strive to have competent personnel, instill an enterprise-wide attitude of integrity and control consciousness, and set a positive corporate direction. These entities establish appropriate controls that foster shared values and teamwork in pursuit of the organization's objectives.

Control environment elements include the following, and the extent to which each element is addressed at SourceOne is described below:

- Management Controls, Philosophy, and Operating Style
- Integrity and Ethical Values
- Organizational Structure
- Assignment of Authority and Responsibility
- Standard Operating Controls
- Audit
- Risk Assessment
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; and setting the tone for the organization. Importance is placed on accuracy and integrity, maintaining written and updated procedures, security and privacy, and establishing and maintaining sound internal controls over all functional aspects of operations.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. SourceOne places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in the daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and regular departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operate under Company policies and procedures, including confidentiality agreements and security policies. Periodic training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring customer base for trends, changes, and anomalies.

Competence should reflect the knowledge and skills needed to accomplish tasks that define an individual's job. Through consideration of an entity's objectives and the strategies and plans for achievement of those objectives, management must determine how well these tasks need to be accomplished. Management has identified the competence levels for particular jobs and translated those levels into requisite knowledge and skills.

Integrity and Ethical Values

Maintaining a climate that demands integrity and ethical values is critical to the establishment and maintenance of an effectively controlled organization. The effectiveness of internal controls cannot rise above the integrity and ethical values of the people who create, administer, and monitor them. SourceOne has programs and policies designed to promote and ensure the integrity and ethical values in its environment.

SourceOne desires to maintain a safe, pleasant, and cooperative working environment and expects employees to have high standards of performance, integrity, productivity, and professionalism. SourceOne has developed professional conduct policies that set forth policies of importance to all employees relating to ethics, values, and conduct. All employees are expected to know and adhere to these standards, as well as to generally accepted norms of conduct and courtesy at all times. While managers are responsible for understanding, communicating, and enforcing Company policies, this does not override or diminish an employee's individual responsibility to be aware of and adhere to these policies. Violations of these policies or other forms of misconduct may lead to disciplinary or corrective action up to and including dismissal.

Standards of Conduct

SourceOne has implemented standards of conduct to guide all employee and contractor behavior. Management monitors behavior closely, and exceptions to these standards lead to immediate corrective action as defined by Human Resources (HR) policies and procedures. Additionally, all employees must sign confidentiality agreements prior to employment. Any employee found to have violated the SourceOne ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

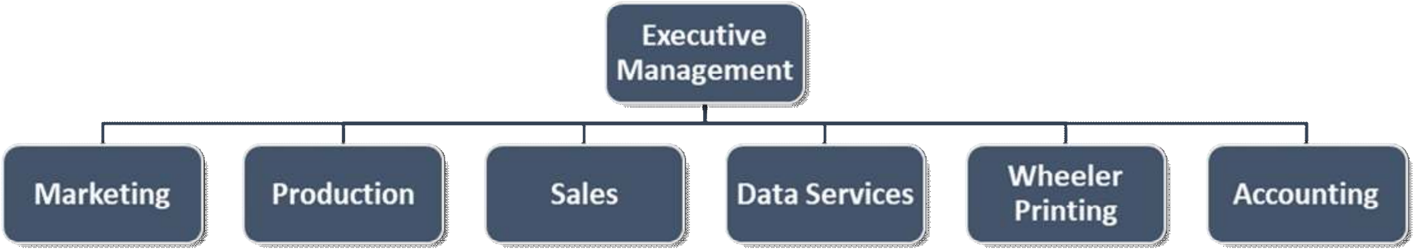
The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set and job requirement. Management monitors and formally evaluates employee and contractor performance on a periodic basis to determine that performance meets or exceeds SourceOne standards.

Organizational Structure

An entity's organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Significant aspects of establishing a relevant organizational structure include defining key areas of authority and responsibility and establishing appropriate lines of reporting. Significant cross-training between management positions and between staff positions exists to help ensure smooth operations and maintenance of controls during staff or management absence.

Roles and Responsibilities

The following organizational chart depicts SourceOne's corporate structure:



Assignment of Authority and Responsibility

The extent to which individuals recognize that they are held accountable influences the control environment. This holds true for everyone who has ultimate responsibility for activities within an entity, including the internal control system. This includes assignment of authority and responsibility for operating activities, and establishment of reporting relationships and authorization protocols. SourceOne management encourages individuals and teams to use initiative in addressing issues and resolving problems. Policies describing appropriate business practices, knowledge and experience of key personnel, and available resources are provided to employees in order to assist them in carrying out their duties.

The Company is led by a team of senior executives that assigns authority and responsibility to key management personnel with the skills and experience necessary to carry out their assignments. Such assignments commonly relate to achieving corporate objectives, oversight of operating functions, and any compliance with applicable regulatory requirements. Open dialogue and individual initiative are encouraged as fundamental parts of the Company's goal to deliver client service.

Executive Management – is responsible for developing and establishing organizational goals, strategic vision, organizational direction, client strategy, client acquisition, market positioning, and Company growth.

Marketing – This department is responsible for listening to customers, understanding the market, executing marketing strategies and building the SourceOne brand, while attracting and tracking products and services demand.

Production – This department is responsible for processing jobs such as lasering, folding, ink jetting, binding, inserting, and metering so all materials are ready to go to the post office for mailing.

Sales – This department is responsible for prospecting for new clients and working with existing clients to produce new and improved methods of reaching the clients' base.

Data Services – This department is responsible for taking all data supplied by the client or third party entities and processing to meet USPS mailing standards.

Wheeler Printing – This separate facility is responsible for non-sensitive print production and bindery/finishing work, as well as graphic design.

Accounting – This department is responsible for day to day accounting procedures. Staff work closely with each department to ensure accurate processes for documenting all expenses are maintained.

Standard Operating Controls

SourceOne Management sends guidance to employees regarding expected levels of integrity, ethical behavior, and competence. Such practices relate to hiring, orientation, training, evaluation, counseling, promotion, compensation, and remedial actions.

HR policies and practices are documented in the employee handbook. The policies and procedures are designed to allow management to recruit, develop, and retain sufficiently competent personnel to achieve SourceOne’s business and control objectives. These objectives include controls and policies for hiring, training, evaluating, promoting, and compensating employees. Employee retention is a high priority, and management clearly establishes and communicates promotion criteria. Management conducts employee performance evaluations or goal reviews on a systematic basis and relates them to SourceOne’s goals.

SourceOne has hiring practices that are designed to help ensure that new employees are qualified for their job responsibilities. All applicants pass through an interview process that assesses their qualifications related to the expected responsibility level of the individual. SourceOne conducts pre-employment reference checks from information provided on the employment application. Additionally, HR conducts pre-hire background investigations relating to past employment history and criminal activity.

SourceOne invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an orientation program that acquaints them with the Company’s organization, its affiliated companies, functions, values, products, and selected policies. Thereafter, development activities include providing more challenging assignments, job rotation, training programs, seminars, and continuing education programs. Additionally, employees are provided with measurable objectives and are subject to periodic performance reviews to help ensure competence.

Security Awareness

SourceOne conducts security training programs for all employees in the areas of physical safety and security. Each member of SourceOne is made aware of the security implications that revolve around their functions and actions. Approaching security as an organization has a more profound effect than relying solely on a single group. This process begins with providing individuals with the understanding and knowledge needed to help secure them and their data within established policies. Security awareness programs include the message that individual users can have a significant impact on the overall security of an organization.

Managers oversee the training and awareness of the topics contained in the Employee Handbook and the Client Security Policy:

- Computer and Email Usage
- Use of Telephones
- Use of Equipment
- Internet Usage Summary Policy
- Computer Software
- Personal Use of Company Property
- Property and Equipment Care
- Restricted Areas
- Return of Company Property
- Safety Rules
- Security Violations of Policies

Audit

SourceOne Management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

SourceOne Senior Management meets on a regular basis to discuss current business and future business opportunities. Items addressed in these meetings pertain to the current risk of the daily business along with potential risks associated with new business opportunities. A review of the business plan may also be performed in these meetings.

SourceOne has a cross functional risk assessment process that utilizes Management, as well as staff, to identify risks that could affect the Company's ability to meet its contractual obligations. Risk assessment efforts include analyses of threats, probabilities of occurrence, potential business impacts, and associated mitigation plans. Risk mitigation strategies include prevention and elimination through the implementation of internal controls and transference through commercial general and umbrella policies. Management maintains risk plans and updates them at least annually.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The Management Team meets regularly to identify any risks and develop corrective steps to minimize the impact of these risks. The Company employs numerous methods to assess and manage risk, including policies, procedures, team structure, recurring meetings, and automated error detection controls. The Company strives to identify and prevent risks at an early stage through policy and procedure adherence in addition to mitigating relevant risks as discovered either through team structure, meetings, or notifications.

The Company maintains security policies and communicates them to staff to ensure that individuals utilizing Company resources understand their responsibility in reducing the risk of compromise and exercise appropriate security measures to protect systems and data.

Monitoring

Management monitors internal controls as part of normal business operations. SourceOne uses a series of management reports and processes to monitor the results of the various business processes. The Management Team regularly reviews the reports and logs, records, and resolves all exceptions to normal processing activities.

The Company uses software to track user and customer requests, which are maintained in a system and tracked until completion. Management performs regular reviews of tasks assigned to their department units. Tasks that are not addressed in a timely manner are manually escalated and resolved.

The Company's Information Technology Team regularly monitors the network for capacity, performance, and hardware failure. Overall system health and capacity planning are monitored daily to ensure the system will meet the needs of the Company's clients. Administrators monitor security access violations, including server logs and reports.

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 administrators use several monitoring tools to identify and provide alerts to the following conditions:

- A managed system has exceeded a predefined performance or load threshold.
- A managed system has suffered an error condition.
- A managed system has detected a hardware element that is expected to fail in the near future.
- A managed system is no longer in communication with the monitoring infrastructure.
- A managed system has entered a condition previously specified by Company administrators as operating outside of a threshold.

Systems Administration utilizes a Web-based resource for performing external vulnerability testing. The assessment includes testing for current and recent known threats against the Company's external-facing Internet firewalls. The testing verifies the configuration of the security policy on the firewall. Detailed reports are delivered upon completion for administrators to act upon if a vulnerability is discovered.

Information and Communication Systems

SourceOne uses a variety of methods for communication to ensure that significant events and issues are conveyed in a timely manner and that staff understand their role and responsibility over service and controls. These methods include the following: new hire training; ongoing training; policy and process updates; weekly departmental meetings summarizing events and changes; the use of email to communicate time sensitive information; and the documentation and storage of historical data in internal repositories for business and support activities. The Company maintains systems that manage the flow of information and facilitate communication with its customers.

Information Flow from Senior Management to Operations Staff

SourceOne has implemented various methods of communication to help ensure that employees understand their individual roles and responsibilities over processing and controls and communicates significant events in a timely manner. Employee manuals are provided upon hire that communicate all policies and procedures concerning employee conduct. Security of the physical premises and logical security of systems is reinforced by training and through awareness programs. The communication system between senior management and operations staff includes the use of the office email system, written memos when appropriate, and weekly meetings. Managers hold departmental meetings with personnel to discuss new Company policies and procedures and other business issues.

Monthly staff and training meetings are utilized to inform staff of new policy and technology updates. Communication is encouraged at all levels to promote the operating efficiency of SourceOne.

Trust Services Criteria and Related Controls

The Company's trust services criteria and related control activities are included in Section III of this report to eliminate the redundancy that would result from listing them here in Section II and repeating them in Section III.

Although the trust services criteria and related control activities are included in Section III, they are, nevertheless, an integral part of Company's description of controls.

Subservice Organizations

SourceOne contracts with FTP Today, Inc. for an enterprise grade file transfer and file sharing software-as-a-service platform which is hosted by Flexential Corp. A current SOC 1 Type 2 report is maintained by FTP Today. A current SOC 2 Type 2 report is maintained by Flexential.

User Control Considerations

SourceOne’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 SourceOne. User auditors should consider whether or not the following controls are implemented at user organizations:

- Controls are in place for user organizations to ensure compliance with contractual requirements.
- Controls are in place 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.
- Controls are in place to provide reasonable assurance of the compatibility of software not provided by SourceOne.
- Controls to provide reasonable assurance that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans (BCP).
- Controls to provide reasonable assurance that SourceOne’s IT is notified in advance of any equipment or other shipments they will be sending or receiving.
- Controls to provide reasonable assurance that confidential systems and information are secured in a best practices manner.
- Controls to provide reasonable assurance of the transmission and receipt of information not provided by SourceOne.
- Controls for approving the telecommunications infrastructure between itself and SourceOne.

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. Providing data center colocation and managed services for customers by SourceOne covers only a portion of the overall internal control structure of each customer. SourceOne’s products and services were not designed to be the only control component in the internal control environment. Additional control procedures require implementation at the customer level. It is not feasible for all of the control objectives relating to providing data center colocation and managed services to be fully achieved by SourceOne. Therefore, each customer’s system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

III. Information Provided by Ascend Audit & Advisory

Common Control Criteria – Security Category

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Environment			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Sets the Tone at the Top—The board of directors and management, at all levels, demonstrate through their directives, actions, and behavior the importance of integrity and ethical values to support the functioning of the system of internal control.	Inspected the most current employee handbook including code of conduct and confidentiality policies, along with the entity's employee confidentiality / HIPAA agreement, to determine Management, at all levels, demonstrated the importance of integrity and ethical values to support the functioning of the system of internal control. Informed by Management a board of directors did not exist during the period under review.	No exceptions noted.
		Establishes Standards of Conduct—The expectations of the board of directors and senior management concerning integrity and ethical values are defined in the entity's standards of conduct and understood at all levels of the entity and by outsourced service providers and business partners.	Inspected the most current employee handbook including code of conduct and confidentiality policies, the entity's employee confidentiality / HIPAA agreement, and an executed business associate agreement to determine standards of conduct were communicated at all levels of the entity and by outsourced service providers and business partners.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Environment (Continued)			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.1 (Cont.)	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Evaluates Adherence to Standards of Conduct—Processes are in place to evaluate the performance of individuals and teams against the entity's expected standards of conduct.	For the selection of active employees, inspected completed employee performance review forms to determine processes were in place to evaluate the performance of individuals against the entity's expected standards of conduct.	No exceptions noted.
		Addresses Deviations in a Timely Manner—Deviations from the entity's expected standards of conduct are identified and remedied in a timely and consistent manner.	Inspected the entity’s employee disciplinary action form and conducted corroborative inquiry of Management to determine deviations from the entity's expected standards of conduct were required to be identified and remedied in a timely and consistent manner. Informed by Management there were no deviations from the entity’s standards of conduct reported during the period under review.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional point of focus specifically related to all engagements using the trust services criteria:				
CC1.1 (Cont.)	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	Considers Contractors and Vendor Employees in Demonstrating Its Commitment—Management and the board of directors consider the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	Inspected the most current employee handbook with respect to contractors, along with an executed business associate agreement, to determine Management, at all levels, considered the use of contractors and vendor employees in its processes for establishing standards of conduct, evaluating adherence to those standards, and addressing deviations in a timely manner.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Environment (Continued)			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.2	COSO Principle 2: The board of directors demonstrates independence from Management and exercises oversight of the development and performance of internal control.	Establishes Oversight Responsibilities—The board of directors identifies and accepts its oversight responsibilities in relation to established requirements and expectations.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.
		Applies Relevant Expertise—The board of directors defines, maintains, and periodically evaluates the skills and expertise needed among its members to enable them to ask probing questions of Senior Management and take commensurate action.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.
		Operates Independently—The board of directors has sufficient members who are independent from Management and objective in evaluations and decision making.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.
Additional point of focus specifically related to all engagements using the trust services criteria:				
		Supplements Board Expertise—The board of directors supplements its expertise relevant to security and availability, as needed, through the use of a subcommittee or consultants.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Considers All Structures of the Entity—Management and the board of directors consider the multiple structures used (including operating units, legal entities, geographic distribution, and outsourced service providers) to support the achievement of objectives.	Inspected documented Management communications with respect to operational and budgetary objectives, along with the most current organizational chart, to determine Management considered the multiple structures used to support the achievement of objectives. Informed by Management a board of directors did not exist during the period under review.	No exceptions noted.
		Establishes Reporting Lines—Management designs and evaluates lines of reporting for each entity structure to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	Inspected documented Management communications with respect to operational and budgetary objectives, along with the most current organizational chart, to determine Management designed and evaluated lines of reporting to enable execution of authorities and responsibilities and flow of information to manage the activities of the entity.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Environment (Continued)			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.3 (Cont.)	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Defines, Assigns, and Limits Authorities and Responsibilities—Management and the board of directors delegate authority, define responsibilities, and use appropriate processes and technology to assign responsibility and segregate duties as necessary at the various levels of the organization.	Inspected documented Management communications with respect to operational and budgetary objectives, along with the most current organizational chart, to determine Management assigned responsibility and segregated duties as necessary at the various levels of the organization.	No exceptions noted.
Additional points of focus specifically related to all engagements using the trust services criteria:				
		Addresses Specific Requirements When Defining Authorities and Responsibilities—Management and the board of directors consider requirements relevant to security and availability when defining authorities and responsibilities.	Inspected documented Management communications with respect to operational and budgetary objectives, along with the entity's most current risk register, to determine Management considered requirements relevant to security and availability when defining authorities and responsibilities.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC1.3 (Cont.)	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Considers Interactions with External Parties When Establishing Structures, Reporting Lines, Authorities, and Responsibilities—Management and the board of directors consider the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	Inspected the most current vendor management policy and procedures, along with an executed business associate agreement, to determine Management considered the need for the entity to interact with and monitor the activities of external parties when establishing structures, reporting lines, authorities, and responsibilities.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Environment (Continued)			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Establishes Policies and Practices—Policies and practices reflect expectations of competence necessary to support the achievement of objectives.	Inspected the most current employee handbook, procedures for evaluating job candidates for employment, new hire onboarding checklist, and the entity's information security and HIPAA training employee attendance records; and for the selection of active employees, inspected executed confidentiality / HIPAA agreements to determine policies and practices reflected expectations of competence necessary to support objectives.	No exceptions noted.
		Evaluates Competence and Addresses Shortcomings—The board of directors and Management evaluate competence across the entity and in outsourced service providers in relation to established policies and practices and act as necessary to address shortcomings.	Inspected the entity's employee disciplinary action form, the most current vendor management policy and procedures, an executed business associate agreement, and conducted corroborative inquiry of Management to determine policies and practices were in place to address shortcomings. Informed by Management a board of directors did not exist during the period under review. Informed by Management there were no competence shortcomings reported during the period under review.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC1.4 (Cont.)	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Attracts, Develops, and Retains Individuals—The entity provides the mentoring and training needed to attract, develop, and retain sufficient and competent personnel and outsourced service providers to support the achievement of objectives.	Inspected procedures for evaluating job candidates for employment, new hire onboarding checklist, and the entity's information security and HIPAA training employee attendance records to determine the entity provided the mentoring and training needed to attract, develop, and retain sufficient and competent personnel to support the achievement of objectives.	No exceptions noted.
		Plans and Prepares for Succession—Senior Management and the board of directors develop contingency plans for assignments of responsibility important for internal control.	Inspected the most current business continuity and disaster recovery plan to determine Senior Management had plans for key positions for internal control.	No exceptions noted.
Additional points of focus specifically related to all engagements using the trust services criteria:				
		Considers the Background of Individuals—The entity considers the background of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	For the population of new employees, inspected completed background check confirmations to determine the entity considered the background of potential employees as a condition of employment.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Environment (Continued)**			
CC1.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC1.4 (Cont.)	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Considers the Technical Competency of Individuals—The entity considers the technical competency of potential and existing personnel, contractors, and vendor employees when determining whether to employ and retain the individuals.	Inspected procedures for evaluating job candidates for employment and for the selection of active employees, inspected completed employee performance review forms to determine the entity considered the technical competency of individuals with respect to employment and career advancement.	No exceptions noted.
		Provides Training to Maintain Technical Competencies—The entity provides training programs, including continuing education and training, to ensure skill sets and technical competency of existing personnel, contractors, and vendor employees are developed and maintained.	Inspected the entity’s information security and HIPAA training attendance records to determine the entity provided training programs to ensure skill sets and technical competency of personnel were developed and maintained.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Environment (Continued)			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Enforces Accountability Through Structures, Authorities, and Responsibilities—Management and the board of directors establish the mechanisms to communicate and hold individuals accountable for performance of internal control responsibilities across the entity and implement corrective action as necessary.	For the selection of active employees, inspected completed employee performance review forms; and for the population of new employees, inspected signed acknowledgments of the employee handbook, along with executed employee confidentiality / HIPAA agreements, to determine individuals were held accountable for performance of internal control responsibilities across the entity. Informed by Management a board of directors did not exist during the period under review.	No exceptions noted.
		Establishes Performance Measures, Incentives, and Rewards—Management and the board of directors establish performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity, reflecting appropriate dimensions of performance and expected standards of conduct, and considering the achievement of both short-term and longer-term objectives.	Inspected the most current employee handbook and for the selection of active employees, inspected completed employee performance review forms to determine Management established performance measures, incentives, and other rewards appropriate for responsibilities at all levels of the entity including short- and longer-term objectives.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Environment (Continued)			
CC1.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC1.5 (Cont.)	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Evaluates Performance Measures, Incentives, and Rewards for Ongoing Relevance—Management aligns incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	Inspected the most current employee handbook and for the selection of active employees, inspected completed employee performance review forms to determine Management aligned incentives and rewards with the fulfillment of internal control responsibilities in the achievement of objectives.	No exceptions noted.
		Considers Excessive Pressures—Management and the board of directors evaluate and adjust pressures associated with the achievement of objectives as they assign responsibilities, develop performance measures, and evaluate performance.	For the selection of active employees, inspected completed employee performance review forms to determine Management evaluated and adjusted pressures associated with the achievement of objectives as they assigned responsibilities, developed performance measures, and evaluated performance.	No exceptions noted.
		Evaluates Performance and Rewards or Disciplines Individuals—Management and the board of directors evaluate performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and provide rewards or exercise disciplinary action, as appropriate.	For the selection of active employees, inspected completed employee performance review forms and inspected the entity's employee disciplinary action form to determine Management evaluated performance of internal control responsibilities, including adherence to standards of conduct and expected levels of competence, and exercised disciplinary action when appropriate.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Communication and Information**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Identifies Information Requirements—A process is in place to identify the information required and expected to support the functioning of the other components of internal control and the achievement of the entity's objectives.	Inspected the shared drive location of the entity's most current system description, policies, procedures, and staff directory, along with the most current risk register and data classification policy and procedures, to determine processes were in place to identify information required and expected to support the system's functioning of internal control and the achievement of the entity's objectives.	No exceptions noted.
		Captures Internal and External Sources of Data—Information systems capture internal and external sources of data.	Inspected connection, authentication, and data transmission logs of the entity's secure file transfer system to determine information systems captured internal and external sources of data.	No exceptions noted.
		Processes Relevant Data into Information—Information systems process and transform relevant data into information.	Inspected logs of successfully completed client statements to determine information systems processed and transformed relevant data into information.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Communication and Information (Continued)			
CC2.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC2.1 (Cont.)	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Maintains Quality Throughout Processing—Information systems produce information that is timely, current, accurate, complete, accessible, protected, verifiable, and retained. Information is reviewed to assess its relevance in supporting the internal control components.	Inspected connection, authentication, and data transmission logs of the entity's secure file transfer system; logs of successfully completed client statements; and the standard operating procedures for remediating associated errors to determine information systems produced information that was timely, accurate, complete, and verifiable per internal controls.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Communication and Information (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Internal Control Information—A process is in place to communicate required information to enable all personnel to understand and carry out their internal control responsibilities.	Inspected the most current information security and incident response policies and procedures, along with the shared drive location of the entity's most current system description, policies, procedures, and staff directory, to determine a process was in place to communicate required information to enable personnel to understand and carry out their internal control responsibilities.	No exceptions noted.
		Communicates with the Board of Directors—Communication exists between Management and the board of directors so that both have information needed to fulfill their roles with respect to the entity's objectives.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.
		Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Inspected the entity's anonymous communication process to determine a separate communication channel existed to serve as a fail-safe mechanism to enable anonymous or confidential communications.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Communication and Information (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the information.	Inspected Management memorandums (i.e., emails) to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine communications considered the timing, audience, and the nature of the information.	No exceptions noted.
Additional points of focus specifically related to all engagements using the trust services criteria:				
		Communicates Responsibilities—Entity personnel with responsibility for designing, developing, implementing, operating, maintaining, or monitoring system controls receive communications about their responsibilities, including changes in their responsibilities, and have the information necessary to carry out those responsibilities.	Inspected Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine personnel received communications about their responsibilities and had information to carry out those responsibilities.	No exceptions noted.
		Communicates Information on Reporting Failures, Incidents, Concerns, and Other Matters—Entity personnel are provided with information on how to report systems failures, incidents, concerns, and other complaints to personnel.	Inspected the most current incident response policy and procedures, along with the entity's anonymous communication process to determine personnel were provided with information on how to report systems failures, incidents, concerns, and other complaints.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Communication and Information (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Objectives and Changes to Objectives—The entity communicates its objectives and changes to those objectives to personnel in a timely manner.	Inspected Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine objectives were communicated in a timely manner.	No exceptions noted.
		Communicates Information to Improve Security Knowledge and Awareness—The entity communicates information to improve security knowledge and awareness and to model appropriate security behaviors to personnel through a security awareness training program.	Inspected the entity's information security and HIPAA training attendance records and for the selection of active employees, inspected executed confidentiality / HIPAA agreements to determine the entity communicated information to improve security knowledge and awareness.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Communication and Information (Continued)**			
CC2.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized personnel to enable them to understand their role in the system and the results of system operation.	Inspected the shared drive location of the entity's most current system description, policies, procedures, and staff directory; and inspected Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine the entity prepared and communicated information about the design and operation of the system to authorized personnel.	No exceptions noted.
		Communicates System Objectives—The entity communicates its objectives to personnel to enable them to carry out their responsibilities.	Inspected the shared drive location of the entity's most current system description, policies, procedures, and staff directory; and inspected Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine the entity communicated objectives to personnel to enable them to carry out responsibilities.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Communication and Information (Continued)			
CC2.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level (continued):				
CC2.2 (Cont.)	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Communicates System Changes—System changes that affect responsibilities or the achievement of the entity's objectives are communicated in a timely manner.	Inspected Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine system changes that affected responsibilities were communicated in a timely manner.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Communication and Information (Continued)			
CC2.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Communicates to External Parties—Processes are in place to communicate relevant and timely information to external parties, including shareholders, partners, owners, regulators, customers, financial analysts, and other external parties.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients, to determine processes were in place to communicate relevant and timely information to external stakeholders.	No exceptions noted.
		Enables Inbound Communications—Open communication channels allow input from customers, consumers, suppliers, external auditors, regulators, financial analysts, and others, providing Management and the board of directors with relevant information.	Inspected the entity's client portal for managing and tracking job orders, along with the entity's online contact information and request submittal interface, to determine communication channels allowed input from external entities for providing Management with relevant information.	No exceptions noted.
		Communicates with the Board of Directors—Relevant information resulting from assessments conducted by external parties is communicated to the Board of Directors and the Management Team.	Informed by Management a board of directors did not exist during the period under review.	No testing performed.
		Provides Separate Communication Lines—Separate communication channels, such as whistle-blower hotlines, are in place and serve as fail-safe mechanisms to enable anonymous or confidential communication when normal channels are inoperative or ineffective.	Inspected the entity's online contact information and request submittal interface to determine separate communication channels were in place to enable anonymous or confidential communication.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Communication and Information (Continued)			
CC2.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC2.3 (Cont.)	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	Selects Relevant Method of Communication—The method of communication considers the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients, to determine communications considered the timing, audience, and nature of the communication and legal, regulatory, and fiduciary requirements and expectations.	No exceptions noted.
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level:				
		Communicates Information About System Operation and Boundaries—The entity prepares and communicates information about the design and operation of the system and its boundaries to authorized external users to permit users to understand their role in the system and the results of system operation.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients; and inspected an executed business associate agreement to determine the entity prepared and communicated information about the design and operation of the system and its boundaries to authorized external users.	No exceptions noted.
		Communicates System Objectives—The entity communicates its system objectives to appropriate external users.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients; and inspected an executed business associate agreement to determine system objectives were communicated to appropriate external users.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Communication and Information (Continued)			
CC2.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
Additional points of focus that apply only when an engagement using the trust services criteria is performed at the system level (continued):				
CC2.3 (Cont.)	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	<u>Communicates System Responsibilities</u>—External users with responsibility for designing, developing, implementing, operating, maintaining, and monitoring system controls receive communications about their responsibilities and have the information necessary to carry out those responsibilities.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients; and inspected an executed business associate agreement to determine external users received communications about their responsibilities and were provided information to carry out those responsibilities.	No exceptions noted.
		<u>Communicates Information on Reporting System Failures, Incidents, Concerns, and Other Matters</u>—External users are provided with information on how to report systems failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the entity's client portal for managing and tracking job orders, along with system generated notifications sent to clients; and inspected an executed business associate agreement to determine external users were provided information on how to report failures, issues, and concerns to appropriate personnel.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Risk Assessment			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Reflects Management's Choices—Operations objectives reflect Management's choices about structure, industry considerations, and performance of the entity.	Inspected the most current risk register, risk management meeting minutes, and Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine operations objectives reflected Management's structure and performance posture.	No exceptions noted.
		Considers Tolerances for Risk—Management considers the acceptable levels of variation relative to the achievement of operations objectives.	Inspected the most current risk register, risk management meeting minutes, and Management memorandums to personnel regarding updates for physical security, operational objectives, and employee roles and responsibilities to determine Management considered acceptable levels of variation relative to the achievement of operations objectives.	No exceptions noted.
		Includes Operations and Financial Performance Goals—The organization reflects the desired level of operations and financial performance for the entity within operations objectives.	Inspected risk management meeting minutes and job control logs, along with documented Management communications with respect to operational and budgetary objectives, to determine the organization reflected operations and business performance within operations objectives.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Forms a Basis for Committing of Resources—Management uses operations objectives as a basis for allocating resources needed to attain desired operations and financial performance.	Inspected documented Management communications with respect to operational and budgetary objectives to determine Management used a formal process for meeting operations and business objectives.	No exceptions noted.
		Complies with Externally Established Frameworks—Management establishes objectives consistent with laws and regulations or standards and frameworks of recognized external organizations.	Inspected an executed business associate agreement, along with the most current SOC reports of the entity's subservice organizations, to determine Management established objectives consistent with standards and frameworks of recognized external organizations.	No exceptions noted.
		Considers the Required Level of Precision—Management reflects the required level of precision and accuracy suitable for user needs and based on criteria established by third parties in nonfinancial reporting.	Inspected the most current SOC reports of the entity's subservice organizations, along with third party vulnerability scan and penetration testing results, to determine Management reflected the required level of precision and accuracy needed to support the entity's commitments and system requirements.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.1 (Cont.)	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	Reflects Entity Activities—External reporting reflects the underlying transactions and events within a range of acceptable limits.	Inspected connection, authentication, and data transmission logs of the entity's secure file transfer system, logs of successfully completed client statements, and the standard operating procedures for remediating associated errors to determine external reporting reflected underlying transactions and events within acceptable limits.	No exceptions noted.
		Reflects External Laws and Regulations—Laws and regulations establish minimum standards of conduct, which the entity integrates into compliance objectives.	Inspected the most current employee handbook including code of conduct and confidentiality policies, along with an executed business associate agreement, to determine the entity established minimum standards of conduct in its compliance objectives.	No exceptions noted.
Additional point of focus specifically related to all engagements using the trust services criteria:				
		Establishes Sub-objectives to Support Objectives—Management identifies sub-objectives related to security and availability to support the achievement of the entity's objectives related to reporting, operations, and compliance.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine Management identified sub-objectives related to security and availability to support the achievement of the entity's objectives related to reporting, operations, and compliance.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Risk Assessment (Continued)			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC3.2	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Includes Entity, Subsidiary, Division, Operating Unit, and Functional Levels—The entity identifies and assesses risk at the entity, subsidiary, division, operating unit, and functional levels relevant to the achievement of objectives.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine the entity identified and assessed risks throughout the organization with respect to the achievement of objectives.	No exceptions noted.
		Analyzes Internal and External Factors—Risk identification considers both internal and external factors and their impact on the achievement of objectives.	Inspected the most current risk register, along with risk management meeting minutes, to determine Management considered internal and external factors and impacts.	No exceptions noted.
		Involves Appropriate Levels of Management—The entity puts into place effective risk assessment mechanisms that involve appropriate levels of Management.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine the entity had effective risk assessment mechanisms that involved appropriate levels of Management.	No exceptions noted.
		Estimates Significance of Risks Identified—Identified risks are analyzed through a process that includes estimating the potential significance of the risk.	Inspected the most current risk register including identified risks and associated risk ratings to determine identified risks were analyzed which included estimating the potential significance of the risks.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Assessment (Continued)			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC3.2 (Cont.)	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Determines How to Respond to Risks—Risk assessment includes considering how the risk should be managed and whether to accept, avoid, reduce, or share the risk.	Inspected the most current risk register including identified risks and associated mitigation strategies to determine Management considered how to manage risks with respect to mitigation strategies.	No exceptions noted.
Additional points of focus specifically related to all engagements using the trust services criteria:				
		Identifies and Assesses Criticality of Information Assets and Identifies Threats and Vulnerabilities—The entity's risk identification and assessment process includes (1) identifying information assets, including physical devices and systems, virtual devices, software, data and data flows, external information systems, and organizational roles; (2) assessing the criticality of those information assets; (3) identifying the threats to the assets from intentional (including malicious) and unintentional acts and environmental events; and (4) identifying the vulnerabilities of the identified assets.	Inspected the most current risk and IT asset inventory registers and internal audit checklist to determine the risk management process identified and assessed threats and vulnerabilities with respect to identified assets.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional points of focus specifically related to all engagements using the trust services criteria (continued):				
CC3.2 (Cont.)	COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	Analyzes Threats and Vulnerabilities from Vendors, Business Partners, and Other Parties—The entity's risk assessment process includes the analysis of potential threats and vulnerabilities arising from vendors providing goods and services, as well as threats and vulnerabilities arising from business partners, customers, and others with access to the entity's information systems.	Inspected the most current risk register and vendor management policy and procedures, along with an executed business associate agreement, to determine the entity’s risk assessment process included analysis of potential threats from vendors and business partners with respect to third party access to the entity’s information systems.	No exceptions noted.
		Considers the Significance of the Risk—The entity’s consideration of the potential significance of the identified risks includes (1) determining the criticality of identified assets in meeting objectives; (2) assessing the impact of identified threats and vulnerabilities in meeting objectives; (3) assessing the likelihood of identified threats; and (4) determining the risk associated with assets based on asset criticality, threat impact, and likelihood.	Inspected the most current risk and IT asset inventory registers to determine the entity’s consideration of the potential significance of the identified risks included: (1) determination of the criticality of identified assets; (2) assessment of impact of identified threats; (3) assessment of the likelihood of identified threats; and (4) determination of the risks associated with assets based on asset criticality, threat impact, and likelihood.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Assessment (Continued)			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Considers Various Types of Fraud—The assessment of fraud considers fraudulent reporting, possible loss of assets, and corruption resulting from the various ways that fraud and misconduct can occur.	Inspected the most current risk and IT asset inventory registers and internal audit checklist to determine fraud was considered as part of risk management objectives.	No exceptions noted.
		Assesses Incentives and Pressures—The assessment of fraud risks considers incentives and pressures.	Inspected the most current risk register and removable media policy which included disposal procedures to determine aspects of fraud were identified as risk objectives.	No exceptions noted.
		Assesses Opportunities—The assessment of fraud risk considers opportunities for unauthorized acquisition, use, or disposal of assets, altering the entity's reporting records, or committing other inappropriate acts.	Inspected the most current risk register and removable media policy which included disposal procedures to determine fraudulent opportunities were considered with respect to disposal of assets.	No exceptions noted.
		Assesses Attitudes and Rationalizations—The assessment of fraud risk considers how Management and other personnel might engage in or justify inappropriate actions.	Inspected the acceptable use policy as contained in the most current employee handbook to determine the assessment of fraud risk considered how Management and other personnel might engage in inappropriate actions.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Assessment (Continued)**			
CC3.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional point of focus specifically related to all engagements using the trust services criteria:				
CC3.3 (Cont.)	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	Considers the Risks Related to the Use of IT and Access to Information—The assessment of fraud risks includes consideration of threats and vulnerabilities that arise specifically from the use of IT and access to information.	Inspected the most current IT asset inventory register and third party vulnerability scan and penetration testing results to determine an assessment of fraud risk included consideration of threats and vulnerabilities from the use of IT and access to information.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Risk Assessment (Continued)			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in the External Environment—The risk identification process considers changes to the regulatory, economic, and physical environment in which the entity operates.	Inspected the most current risk register and physical access and security policy as contained in the most current information security policy and procedures, along with a Management memorandum to personnel regarding updates for physical security, to determine the risk assessment process considered changes to external factors and the entity's physical environment.	No exceptions noted.
		Assesses Changes in the Business Model—The entity considers the potential impacts of new business lines, dramatically altered compositions of existing business lines, acquired or divested business operations on the system of internal control, rapid growth, changing reliance on foreign geographies, and new technologies.	Inspected the most current risk register, along with documented Management communications with respect to operational and budgetary objectives, to determine Management considered potential impacts to the business with respect to lines of business and business operations.	No exceptions noted.
		Assesses Changes in Leadership—The entity considers changes in Management and respective attitudes and philosophies on the system of internal control.	Inspected documented Management communications with respect to operational and budgetary objectives, along with risk management meeting minutes, to determine Management considered material changes in Management and respective attitudes and philosophies on the system of internal control.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Assessment (Continued)			
CC3.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
Additional points of focus specifically related to all engagements using the trust services criteria:				
CC3.4 (Cont.)	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	Assesses Changes in Systems and Technology—The risk identification process considers changes arising from changes in the entity's systems and changes in the technology environment.	Inspected the most current risk register, documented Management communications with respect to operational and budgetary objectives, and risk management meeting minutes to determine the risk assessment process considered changes with respect to the entity's systems and changes to the technology environment.	No exceptions noted.
		Assesses Changes in Vendor and Business Partner Relationships—The risk identification process considers changes in vendor and business partner relationships.	Inspected the most current risk register and vendor management policy and procedures to determine the risk assessment process considered changes in vendor and business partner relationships.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Monitoring Activities			
CC4.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC4.1	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Considers a Mix of Ongoing and Separate Evaluations—Management includes a balance of ongoing and separate evaluations.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators and system generated event logging and notifications; and inspected third party vulnerability scan and penetration testing results, to determine Management included a balance of ongoing and separate evaluations.	No exceptions noted.
		Considers Rate of Change—Management considers the rate of change in business and business processes when selecting and developing ongoing and separate evaluations.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators, and system generated event logging and notifications; and inspected risk management meeting minutes to determine Management considered the rate of change in business processes.	No exceptions noted.
		Establishes Baseline Understanding—The design and current state of an internal control system are used to establish a baseline for ongoing and separate evaluations.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators, and system generated event logging and notifications; and inspected the most current risk register and third party vulnerability scan and penetration testing results to determine the design and current state of the internal control system was utilized to establish a baseline for system evaluations.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC4.1 (Cont.)	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Uses Knowledgeable Personnel—Evaluators performing ongoing and separate evaluations have sufficient knowledge to understand what is being evaluated.	Inspected the entity's most current IT security job description to determine system evaluators had sufficient knowledge to understand what was being evaluated.	No exceptions noted.
		Integrates with Business Processes—Ongoing evaluations are built into the business processes and adjust to changing conditions.	Inspected the most current risk register and internal audit checklist, third party vulnerability scan and penetration testing results, and risk management meeting minutes to determine ongoing evaluations were built into processes with respect to adjustments to changing conditions.	No exceptions noted.
		Adjusts Scope and Frequency—Management varies the scope and frequency of separate evaluations depending on risk.	Inspected the most current risk register, internal audit checklist, and risk management meeting minutes to determine Management monitored the scope and frequency of separate evaluations depending on risk.	No exceptions noted.
		Objectively Evaluates—Separate evaluations are performed periodically to provide objective feedback.	Inspected third party vulnerability scan and penetration testing results to determine separate evaluations were performed periodically for objective feedback.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Monitoring Activities (Continued)**			
CC4.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
Additional point of focus specifically related to all engagements using the trust services criteria:				
CC4.1 (Cont.)	COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Considers Different Types of Ongoing and Separate Evaluations—Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certification made against established specifications (for example, ISO certifications), and internal audit assessments.	Inspected the most current risk register and internal audit checklist, along with third party vulnerability scan and penetration testing results, to determine Management used various types of ongoing and separate evaluations and internal audit assessments.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Monitoring Activities (Continued)			
CC4.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC4.2	COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including Senior Management and the board of directors, as appropriate.	Assesses Results—Management and the board of directors, as appropriate, assess results of ongoing and separate evaluations.	Inspected risk management meeting minutes to determine Management assessed results of ongoing and separate evaluations. Informed by Management a board of directors did not exist during the period under review.	No exceptions noted.
		Communicates Deficiencies—Deficiencies are communicated to parties responsible for taking corrective action and to Senior Management and the board of directors, as appropriate.	Inspected a completed nonconformity report for a reported nonconformance, along with completed client job orders and associated communications, to determine deficiencies were communicated to parties responsible for taking corrective action and to Senior Management.	No exceptions noted.
		Monitors Corrective Action—Management tracks whether deficiencies are remedied on a timely basis.	Inspected a completed nonconformity report for a reported nonconformance, along with completed client job orders and associated communications, to determine Management tracked deficiencies remediation on a timely basis.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Activities			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.1	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Integrates with Risk Assessment—Control activities help ensure that risk responses that address and mitigate risks are carried out.	Inspected the most current risk register, completed disaster recovery testing results, and server hardening guidelines adopted by IT Management to determine control activities helped ensure risk mitigation was carried out.	No exceptions noted.
		Considers Entity-Specific Factors—Management considers how the environment, complexity, nature, and scope of its operations, as well as the specific characteristics of its organization, affect the selection and development of control activities.	Inspected the most current risk register, along with risk management meeting minutes, to determine Management considered entity-specific factors for the selection and development of control activities.	No exceptions noted.
		Determines Relevant Business Processes—Management determines which relevant business processes require control activities.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine Management identified relevant business processes that required control activities.	No exceptions noted.
		Evaluates a Mix of Control Activity Types—Control activities include a range and variety of controls and may include a balance of approaches to mitigate risks, considering both manual and automated controls, and preventive and detective controls.	Inspected the most current risk register, internal audit checklist, third party vulnerability scan and penetration testing results, and risk management meeting minutes to determine Management evaluated a mix of control activity types with respect to risk mitigation.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Control Activities (Continued)**			
CC5.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC5.1 (Cont.)	COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	Considers at What Level Activities Are Applied—Management considers control activities at various levels in the entity.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine Management considered control activities at various levels in the entity.	No exceptions noted.
		Addresses Segregation of Duties—Management segregates incompatible duties, and where such segregation is not practical, Management selects and develops alternative control activities.	Inspected completed client job orders and associated communications to determine segregation of duties was utilized as a control activity for incompatible duties.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Control Activities (Continued)			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Determines Dependency Between the Use of Technology in Business Processes and Technology General Controls—Management understands and determines the dependency and linkage between business processes, automated control activities, and technology general controls.	Inspected the most current risk register, documented Management communications with respect to operational and budgetary objectives, and risk management meeting minutes to determine Management considered dependencies and linkage between business processes and various control activities.	No exceptions noted.
		Establishes Relevant Technology Infrastructure Control Activities—Management selects and develops control activities over the technology infrastructure, which are designed and implemented to help ensure the completeness, accuracy, and availability of technology processing.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators, and system generated event logging and notifications; and inspected logs of successfully completed client statements, along with completed disaster recovery testing results, to determine Management developed and implemented control activities to help ensure complete, accurate, and available technology processing.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Activities (Continued)			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.2 (Cont.)	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	Establishes Relevant Security Management Process Controls Activities—Management selects and develops control activities that are designed and implemented to restrict technology access rights to authorized users commensurate with their job responsibilities and to protect the entity's assets from external threats.	Inspected the most current risk register and internal audit checklist, along with completed network access rights reviews, to determine Management implemented control activities to restrict access rights with respect to appropriateness of user job functions and protected assets from external threats.	No exceptions noted.
		Establishes Relevant Technology Acquisition, Development, and Maintenance Process Control Activities—Management selects and develops control activities over the acquisition, development, and maintenance of technology and its infrastructure to achieve management's objectives.	Inspected the process and Management communications regarding forecasted production equipment expenditures to determine Management implemented control activities with respect to the development and maintenance of technology and infrastructure.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Activities (Continued)			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Establishes Policies and Procedures to Support Deployment of Management's Directives—Management establishes control activities that are built into business processes and employees' day-to-day activities through policies establishing what is expected and relevant procedures specifying actions.	Inspected the most current information security and incident response policies and procedures, a completed nonconformity report for a reported nonconformance, and completed client job orders and associated communications to determine Management established control activities that were built into business processes establishing what was expected and procedures specifying actions.	No exceptions noted.
		Establishes Responsibility and Accountability for Executing Policies and Procedures—Management establishes responsibility and accountability for control activities with management (or other designated personnel) of the business unit or function in which the relevant risks reside.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine Management established responsibility and accountability for control activities of the business function in which associated risks resided.	No exceptions noted.
		Performs in a Timely Manner—Responsible personnel perform control activities in a timely manner as defined by the policies and procedures.	Inspected a completed nonconformity report for a reported nonconformance, along with completed client job orders and associated communications, to determine responsible personnel performed control activities in a timely manner per policy and procedures.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Control Activities (Continued)			
CC5.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC5.3 (Con.t)	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Takes Corrective Action—Responsible personnel investigate and act on matters identified as a result of executing control activities.	Inspected a completed nonconformity report for a reported nonconformance, along with completed client job orders and associated communications, to determine personnel took action on matters identified as a result of executing control activities.	No exceptions noted.
		Performs Using Competent Personnel—Competent personnel with sufficient authority perform control activities with diligence and continuing focus.	Inspected the entity's most current IT security job description, along with risk management meeting minutes, to determine appropriate personnel performed control activities per control activity objectives.	No exceptions noted.
		Reassesses Policies and Procedures—Management periodically reviews control activities to determine their continued relevance and refreshes them when necessary.	Inspected the most current risk register and internal audit checklist, along with risk management meeting minutes, to determine Management periodically reviewed control activities for continued relevance or adjustments.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Logical and Physical Access Controls			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Identifies and Manages the Inventory of Information Assets—The entity identifies, inventories, classifies, and manages information assets.	Inspected the most current IT asset inventory register and data classification policy and procedures to determine the entity identified, inventoried, classified, and managed information assets.	No exceptions noted.
		Restricts Logical Access—Logical access to information assets, including hardware, data (at-rest, during processing, or in transmission), software, administrative authorities, mobile devices, output, and offline system components is restricted through the use of access control software and rule sets.	Observed via walkthrough procedures, the authorized user access control list and security group configurations of the entity's network operating system; and inspected the cloud based remote user access software configuration to determine logical access to information assets was restricted through the use of access control software and rule sets.	No exceptions noted.
		Identifies and Authenticates Users—Persons, infrastructure, and software are identified and authenticated prior to accessing information assets, whether locally or remotely.	Observed via walkthrough procedures, the authorized user access control list and security group configurations of the entity's network operating system; and inspected the cloud based remote user access software configuration to determine personnel and the system were identified and authenticated prior to accessing information assets.	No exceptions noted.
		Considers Network Segmentation—Network segmentation permits unrelated portions of the entity's information system to be isolated from each other.	Inspected the most current network topology and customer data flow and custody diagrams to determine the network was segmented for critical system isolation.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC6.1 (Cont.)	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.	Manages Points of Access—Points of access by outside entities and the types of data that flow through the points of access are identified, inventoried, and managed. The types of individuals and systems using each point of access are identified, documented, and managed.	Observed via walkthrough procedures, the firewall system management interface, access route rules, and system generated event logging and notifications; and inspected domain event logging from the entity's network operating system, along with the entity's cloud based remote user access software configuration, to determine points of access and the types of users were identified, logged, and managed.	No exceptions noted.
		Restricts Access to Information Assets—Combinations of data classification, separate data structures, port restrictions, access protocol restrictions, user identification, and digital certificates are used to establish access control rules for information assets.	Observed via walkthrough procedures, the access route rules of the entity's firewall system, along with the authorized user access control list and security group configurations of the entity's network operating system; and inspected the cloud based remote user access software configuration to determine the entity utilized a combination of access controls that restricted access to information assets.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC6.1 (Cont.)	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.	Manages Identification and Authentication—Identification and authentication requirements are established, documented, and managed for individuals and systems accessing entity information, infrastructure, and software.	Observed via walkthrough procedures, the authorized user access control list, security group configurations, and password policy of the entity’s network operating system; and inspected the cloud based remote user access software configuration to determine identification and authentication requirements were established and managed for personnel and systems.	No exceptions noted.
		Manages Credentials for Infrastructure and Software—New internal and external infrastructure and software users are registered, authorized, and documented prior to being granted access credentials and implemented on the network or access point. Credentials are removed and access is disabled when access is no longer required, or the infrastructure and software are no longer in use.	Inspected the entity’s new employee onboarding checklist to determine new users were required to be registered, authorized, and documented prior to network access provisioning. Informed by Management there were no new network access requests required or provisioned during the period under review.	No exceptions noted.
			For the population of terminated employees provisioned with network access, inspected completed employee termination checklists to determine removal of access was disabled when no longer required.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC6.1 (Cont.)	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.	Uses Encryption to Protect Data—The entity uses encryption to supplement other measures used to protect data-at-rest, when such protections are deemed appropriate based on assessed risk.	Inspected the encryption settings for shared and local drives of the entity’s storage drive encryption system to determine the entity utilized encryption to protect data-at-rest.	No exceptions noted.
		Protects Encryption Keys—Processes are in place to protect encryption keys during generation, storage, use, and destruction.	Inspected the encryption recovery key directory of the entity’s storage drive encryption system to determine processes were in place to protect the security of encryption keys.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Controls Access Credentials to Protected Assets—Information asset access credentials are created based on an authorization from the system's asset owner or authorized custodian.	Inspected the entity's new employee onboarding checklist to determine access credentials were required to be created based on an authorization from associated stakeholders. Informed by Management there were no new network access requests required or provisioned during the period under review.	No exceptions noted.
		Removes Access to Protected Assets When Appropriate—Processes are in place to remove credential access when an individual no longer requires such access.	For the population of terminated employees provisioned with network access, inspected completed employee termination checklists to determine removal of access was required to be disabled when no longer required.	No exceptions noted.
		Reviews Appropriateness of Access Credentials—The appropriateness of access credentials is reviewed on a periodic basis for unnecessary and inappropriate individuals with credentials.	Inspected completed network access rights reviews to determine access credentials were reviewed on a periodic basis for appropriateness.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Creates or Modifies Access to Protected Information Assets—Processes are in place to create or modify access to protected information assets based on authorization from the asset's owner.	Inspected the entity's new employee onboarding checklist to determine processes were in place to create access to protected information assets based on authorization from asset owners. Informed by Management there were no new network access requests required or provisioned during the period under review.	No exceptions noted.
		Removes Access to Protected Information Assets—Processes are in place to remove access to protected information assets when an individual no longer requires access.	For the population of terminated employees provisioned with network access, inspected completed employee termination checklists to determine removal of access was required to be disabled when no longer required.	No exceptions noted.
		Uses Role-Based Access Controls—Role-based access control is utilized to support segregation of incompatible functions.	Observed via walkthrough procedures, the security group configurations of the entity's network operating system to determine role-based access control was utilized to support segregation of incompatible functions.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity’s objectives.	Creates or Modifies Physical Access—Processes are in place to create or modify physical access to facilities such as data centers, office spaces, and work areas, based on authorization from the system's asset owner.	Inspected the physical access and security policy as contained in the most current information security policy and procedures, and for the population of new employees, inspected completed new hire checklists to determine processes were in place to create physical access to facilities based on authorization from system asset owners.	No exceptions noted.
		Removes Physical Access—Processes are in place to remove access to physical resources when an individual no longer requires access.	For the population of terminated employees provisioned physical access, inspected completed employee termination checklists to determine removal of physical access was disabled when no longer required.	No exceptions noted.
		Reviews Physical Access—Processes are in place to periodically review physical access to ensure consistency with job responsibilities.	Inspected the most current physical access rights review, along with a Management memorandum to personnel regarding updates for physical security, to determine processes were in place to periodically review physical access for appropriateness.	No exceptions noted.

-

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Identifies Data and Software for Disposal—Procedures are in place to identify data and software stored on equipment to be disposed and to render such data and software unreadable.	Inspected the most current risk register and removable media policy which included disposal procedures to determine procedures were in place to identify data and software on equipment to be disposed and to render such data and software unreadable.	No exceptions noted.
		Removes Data and Software from Entity Control—Procedures are in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	Inspected the most current risk register and removable media policy which included disposal procedures to determine procedures were in place to remove data and software stored on equipment to be removed from the physical control of the entity and to render such data and software unreadable.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	Restricts Access—The types of activities that can occur through a communication channel (for example, FTP site, router port) are restricted.	Observed via walkthrough procedures, the firewall access route rules of the entity's firewall system; and inspected the entity's cloud based remote user access software configuration to determine types of activities through communication channels were restricted.	No exceptions noted.
		Protects Identification and Authentication Credentials—Identification and authentication credentials are protected during transmission outside its system boundaries.	Inspected the entity's cloud based remote user access software configuration, along with a Management memorandum to personnel mandating multi-factor authentication activation for email accounts, to determine identification and authentication credentials were protected.	No exceptions noted.
		Requires Additional Authentication or Credentials—Additional authentication information or credentials are required when accessing the system from outside its boundaries.	Inspected a Management memorandum to personnel mandating multi-factor authentication activation for email accounts to determine additional authentication credentials were required when accessing the system from outside its boundaries.	No exceptions noted.

<table>
<tr><th></th><th colspan="4">TRUST SERVICES CRITERIA AND POINTS OF FOCUS</th></tr>
<tr><th>TSC REF #</th><th colspan="4">Logical and Physical Access Controls (Continued)</th></tr>
<tr><th>CC6.0</th><th>Trust Services Criteria for the Security Category</th><th>Description of Points of Focus</th><th>Ascend Audit & Advisory Tests of Points of Focus</th><th>Test Results</th></tr>
<tr><td>CC6.6 (Cont.)</td><td>The entity implements logical access security measures to protect against threats from sources outside its system boundaries.</td><td><u>Implements Boundary Protection Systems</u>—Boundary protection systems (for example, firewalls, demilitarized zones, and intrusion detection systems) are implemented to protect external access points from attempts and unauthorized access and are monitored to detect such attempts.</td><td>Observed via walkthrough procedures, the entity’s firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine boundary protection systems were implemented to protect external access points from unauthorized access and access attempts were monitored.</td><td>No exceptions noted.</td></tr>
</table>

	Trust Services Criteria and Points of Focus			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Restricts the Ability to Perform Transmission—Data loss prevention processes and technologies are used to restrict ability to authorize and execute transmission, movement, and removal of information.	Inspected the data loss prevention management interface including system activity metrics to determine data loss prevention processes and technologies were utilized to restrict the ability to authorize and execute transmission, movement, and removal of information.	No exceptions noted.
		Uses Encryption Technologies or Secure Communication Channels to Protect Data—Encryption technologies or secured communication channels are used to protect transmission of data and other communications beyond connectivity access points.	Inspected the entity's cloud based remote user access software encryption configuration to determine encryption technologies were utilized to protect transmission of data.	No exceptions noted.
		Protects Removable Media—Encryption technologies and physical asset protections are used for removable media (such as USB drives and backup tapes), as appropriate.	Inspected the most current removable media policy and procedures, along with the encryption settings for shared and local drives of the entity's storage drive encryption system, to determine encryption technologies and physical protections were utilized for removable media.	No exceptions noted.
		Protects Mobile Devices—Processes are in place to protect mobile devices (such as laptops, smart phones, and tablets) that serve as information assets.	Informed by Management the entity did not utilize mobile devices serving as information assets during the period under review.	No testing performed.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Logical and Physical Access Controls (Continued)**			
CC6.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Restricts Application and Software Installation—The ability to install applications and software is restricted to authorized individuals.	Observed via walkthrough procedures, the local domain administrator security group, properties and membership of the entity's network operating system; and inspected the acceptable use policy as contained in the most current employee handbook to determine the ability to install applications and software was restricted to authorized personnel.	No exceptions noted.
		Detects Unauthorized Changes to Software and Configuration Parameters—Processes are in place to detect changes to software and configuration parameters that may be indicative of unauthorized or malicious software.	Observed via walkthrough procedures, the threat detection and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine processes were in place to detect configuration parameters that could be indicative of unauthorized software and malicious software.	No exceptions noted.
		Uses a Defined Change Control Process—A management-defined change control process is used for the implementation of software.	Informed by Management the entity did not engage in software development activities during the period under review.	No testing performed.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	Logical and Physical Access Controls (Continued)			
CC6.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC6.8 (Cont.)	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	Uses Anti-virus and Anti-Malware Software—Anti-virus and anti-malware software is implemented and maintained to provide for the interception or detection and remediation of malware.	Observed via walkthrough procedures, the anti-virus software management interface, endpoints protected, polling schedule for new threat definition, endpoint scanning frequency configuration, and system generated event notifications to determine anti-virus software was implemented and maintained.	No exceptions noted.
		Scans Information Assets from Outside the Entity for Malware and Other Unauthorized Software—Procedures are in place to scan information assets that have been transferred or returned to the entity's custody for malware and other unauthorized software and to remove any items detected prior to its implementation on the network.	Observed via walkthrough procedures, the anti-virus software management interface, endpoints protected, endpoint scanning frequency configuration, and system generated event notifications to determine the anti-virus system scanned production information assets for malware and unauthorized software installations.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Uses Defined Configuration Standards—Management has defined configuration standards.	Inspected the entity's most current job control (i.e., change management) policy and procedures for creating and managing customer job orders, along with server hardening guidelines adopted by IT Management, to determine Management had defined configuration standards.	No exceptions noted.
		Monitors Infrastructure and Software—The entity monitors infrastructure and software for noncompliance with the standards, which could threaten the achievement of the entity's objectives.	Observed via walkthrough procedures, the network and server monitoring, firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine the entity monitored infrastructure and software for noncompliance with standards.	No exceptions noted.
		Implements Change-Detection Mechanisms—The IT system includes a change-detection mechanism (for example, file integrity monitoring tools) to alert personnel to unauthorized modifications of critical system files, configuration files, or content files.	Observed via walkthrough procedures, the threat detection and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine the IT system had change-detection mechanisms to alert personnel to unauthorized modifications of the system.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC7.1 (Cont.)	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.	Detects Unknown or Unauthorized Components—Procedures are in place to detect the introduction of unknown or unauthorized components.	Observed via walkthrough procedures, the network and server monitoring, firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine procedures were in place to detect the introduction of unauthorized components.	No exceptions noted.
		Conducts Vulnerability Scans—The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.	Inspected third party vulnerability scan and penetration testing results to determine the entity conducted vulnerability scans to identify potential vulnerabilities.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Implements Detection Policies, Procedures, and Tools—Detection policies and procedures are defined and implemented, and detection tools are implemented on Infrastructure and software to identify anomalies in the operation or unusual activity on systems. Procedures may include (1) a defined governance process for security event detection and management that includes provision of resources; (2) use of intelligence sources to identify newly discovered threats and vulnerabilities; and (3) logging of unusual system activities.	Inspected the most current incident response policy and procedures to determine detection policies and procedures were defined for security event detection. Observed via walkthrough procedures, the firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine the entity utilized detection tools for the discovery and logging of threats and vulnerabilities.	No exceptions noted.
		Designs Detection Measures—Detection measures are designed to identify anomalies that could result from actual or attempted (1) compromise of physical barriers; (2) unauthorized actions of authorized personnel; (3) use of compromised identification and authentication credentials; (4) unauthorized access from outside the system boundaries; (5) compromise of authorized external parties; and (6) implementation or connection of unauthorized hardware and software.	Observed via walkthrough procedures, the network and server monitoring, firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications, to determine detection measures were designed to identify anomalies that could result in security threats.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.2 (Cont.)	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.	Implements Filters to Analyze Anomalies—Management has implemented procedures to filter, summarize, and analyze anomalies to identify security events.	Observed via walkthrough procedures, the network and server monitoring, firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications; and inspected risk management meeting minutes to determine Management implemented procedures to process anomalies to identify security events.	No exceptions noted.
		Monitors Detection Tools for Effective Operation—Management has implemented processes to monitor the effectiveness of detection tools.	Observed via walkthrough procedures, the network and server monitoring, firewall, threat detection, and anti-virus management interfaces, along with associated system generated event logging and notifications; and inspected risk management meeting minutes to determine Management implemented processes to monitor the effectiveness of detection tools.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Responds to Security Incidents—Procedures are in place for responding to security incidents and evaluating the effectiveness of those policies and procedures on a periodic basis.	Inspected the most current incident response policy and procedures and risk register to determine procedures were in place for responding to security incidents and evaluating the effectiveness of policy and procedures.	No exceptions noted.
		Communicates and Reviews Detected Security Events—Detected security events are communicated to and reviewed by the individuals responsible for the management of the security program and actions are taken, if necessary.	Observed via walkthrough procedures, the threat detection and anti-virus management interfaces, along with associated system generated event notifications; and inspected risk management meeting minutes to determine detected security events were communicated and reviewed by security Management and actions were taken when necessary.	No exceptions noted.
		Develops and Implements Procedures to Analyze Security Incidents—Procedures are in place to analyze security incidents and determine system impact.	Inspected the most current incident response policy and procedures to determine procedures were in place to analyze security incidents and identify system impact. Informed by Management there were no security incidents reported during the period under review.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
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.	Assigns Roles and Responsibilities—Roles and responsibilities for the design, implementation, maintenance, and execution of the incident response program are assigned, including the use of external resources when necessary.	Inspected the most current incident response policy and procedures to determine roles and responsibilities for the program were assigned.	No exceptions noted.
		Contains Security Incidents—Procedures are in place to contain security incidents that actively threaten entity objectives.	Inspected the most current incident response policy and procedures to determine procedures were in place to contain security incidents. Informed by Management there were no security incidents reported during the period under review.	No exceptions noted.
		Mitigates Ongoing Security Incidents—Procedures are in place to mitigate the effects of ongoing security incidents.	Inspected the most current incident response policy and procedures and risk register, along with risk management meeting minutes, to determine procedures were in place to mitigate the effects of ongoing security incidents.	No exceptions noted.
		Ends Threats Posed by Security Incidents—Procedures are in place to end the threats posed by security incidents through closure of the vulnerability, removal of unauthorized access, and other remediation actions.	Inspected the most current incident response policy and procedures and risk register, along with risk management meeting minutes, to determine procedures were in place to end threats from security incidents through remediation actions.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Restores Operations—Procedures are in place to restore data and business operations to an interim state that permits the achievement of entity objectives.	Inspected the entity’s cloud based data backup management interface and backup schedules, along with a completed data restore request, to determine procedures were in place to restore data and business operations.	No exceptions noted.
		Develops and Implements Communication Protocols for Security Incidents—Protocols for communicating security incidents and actions taken to affected parties are developed and implemented to meet the entity's objectives.	Inspected the most current incident response policy and procedures to determine protocols for communicating security incidents and actions to be taken were developed and implemented.	No exceptions noted.
		Obtains Understanding of Nature of Incident and Determines Containment Strategy—An understanding of the nature (for example, the method by which the incident occurred and the affected system resources) and severity of the security incident is obtained to determine the appropriate containment strategy, including (1) a determination of the appropriate response time frame, and (2) the determination and execution of the containment approach.	Inspected the most current incident response policy and procedures to determine the nature and severity of security incidents was required to be evaluated for appropriate containment strategies.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Remediates Identified Vulnerabilities—Identified vulnerabilities are remediated through the development and execution of remediation activities.	Inspected a completed nonconformity report for a reported nonconformance, completed client job orders and associated communications, and risk management meeting minutes to determine identified vulnerabilities were remediated through the development and execution of remediation activities.	No exceptions noted.
		Communicates Remediation Activities—Remediation activities are documented and communicated in accordance with the incident response program.	Inspected a completed nonconformity report for a reported nonconformance, completed client job orders and associated communications, and risk management meeting minutes to determine remediation activities were documented and communicated in accordance with policy.	No exceptions noted.
		Evaluates the Effectiveness of Incident Response—The design of incident response activities is evaluated for effectiveness on a periodic basis.	Inspected the most current incident response policy and procedures and risk register, along with risk management meeting minutes, to determine the design of the incident response activities was evaluated for effectiveness on a periodic basis.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**System Operations (Continued)**			
CC7.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC7.4 (Cont.)	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Periodically Evaluates Incidents—Periodically, management reviews incidents related to security and availability and identifies the need for system changes based on incident patterns and root causes.	Observed via walkthrough procedures, the threat detection and anti-virus management interfaces, along with associated system generated event logging and notifications; and inspected risk management meeting minutes to determine Management reviewed events related to security and availability with respect to needed changes to the system, on a periodic basis.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	Restores the Affected Environment—The activities restore the affected environment to functional operation by rebuilding systems, updating software, installing patches, and changing configurations, as needed.	Inspected completed disaster recovery testing results, a completed data restore request, and logs of installed patch updates to determine activities were in place to rebuild systems, update software, install patches, and change configurations as needed.	No exceptions noted.
		Communicates Information About the Event—Communications about the nature of the incident, recovery actions taken, and activities required for the prevention of future security events are made to management and others as appropriate (internal and external).	Inspected the most current incident response policy and procedures and conducted corroborative inquiry of IT Management to determine communications of incident details were required to be made to Management and associated stakeholders. Informed by Management there were no security incidents reported during the period under review.	No exceptions noted.
		Determines Root Cause of the Event—The root cause of the event is determined.	Inspected a completed nonconformity report for a reported nonconformance to determine the root cause of the event was determined.	No exceptions noted.

TSC REF #	Trust Services Criteria and Points of Focus			
	System Operations (Continued)			
CC7.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC7.5 (Cont.)	The entity identifies, develops, and implements activities to recover from identified security incidents.	Implements Changes to Prevent and Detect Recurrences—Additional architecture or changes to preventive and detective controls, or both, are implemented to prevent and detect recurrences on a timely basis.	Observed via walkthrough procedures, the threat detection and anti-virus management interfaces, along with associated system generated event logging and notifications; and inspected risk management meeting minutes to determine changes to preventive and detective controls were implemented on a timely basis.	No exceptions noted.
		Improves Response and Recovery Procedures—Lessons learned are analyzed, and the incident response plan and recovery procedures are improved.	Inspected a completed nonconformity report for a reported nonconformance to determine lessons learned were analyzed with respect to incident response plan and process improvement.	No exceptions noted.
		Implements Incident Recovery Plan Testing—Incident recovery plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of relevant system components from across the entity that can impair availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Inspected completed disaster recovery testing results, along with a completed data restore request, to determine incident recovery plan testing was performed on a periodic basis.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
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.	Manages Changes Throughout the System Lifecycle—A process for managing system changes throughout the lifecycle of the system and its components (infrastructure, data, software, and procedures) is used to support system availability and processing integrity.	Inspected the entity's most current job control policy and procedures, client portal for managing and tracking job orders including completed orders and associated communications, and a completed nonconformity report for a reported nonconformance to determine a process for managing system changes throughout the lifecycle of the system was utilized to support system availability and processing integrity. Informed by Management the entity did not engage in software development activities during the period under review.	No exceptions noted.
		Authorizes Changes—A process is in place to authorize system changes prior to implementation.	Inspected the entity's most current job control policy and procedures, client portal for managing and tracking job orders including completed orders and associated communications, and a completed nonconformity report for a reported nonconformance to determine a formal process was in place to authorize system changes prior to implementation.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Designs and Develops Changes—A process is in place to design and develop system changes.	Inspected the entity's most current job control policy and procedures, client portal for managing and tracking job orders including completed orders and associated communications, and a completed nonconformity report for a reported nonconformance to determine a process was in place to design and develop system changes.	No exceptions noted.
		Documents Changes—A process is in place to document system changes to support ongoing maintenance of the system and to support system users in performing their responsibilities.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine a process was in place to document system changes with respect to support of ongoing maintenance and system user responsibilities.	No exceptions noted.
		Tracks System Changes—A process is in place to track system changes prior to implementation.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine a process was in place to track system changes prior to implementation.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
TSC REF #	**Change Management (Continued)**			
CC8.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Configures Software—A process is in place to select and implement the configuration parameters used to control the functionality of software.	Inspected a completed nonconformity report for a reported nonconformance to determine a process was in place to select and implement configuration parameters used to control software functionality.	No exceptions noted.
		Tests System Changes—A process is in place to test system changes prior to implementation.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine a process was in place to test system changes prior to implementation.	No exceptions noted.
		Approves System Changes—A process is in place to approve system changes prior to implementation.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine a process was in place to approve system changes prior to implementation.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Change Management (Continued)			
CC8.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Deploys System Changes—A process is in place to implement system changes.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine a process was in place to implement system changes.	No exceptions noted.
		Identifies and Evaluates System Changes—Objectives affected by system changes are identified, and the ability of the modified system to meet the objectives is evaluated throughout the system development life cycle.	Inspected the entity's client portal for managing and tracking job orders including completed orders and associated communications, along with a completed nonconformity report for a reported nonconformance, to determine objectives for system changes were identified and the ability to modify objectives was evaluated throughout the change management process.	No exceptions noted.
		Identifies Changes in Infrastructure, Data, Software, and Procedures Required to Remediate Incidents—Changes in infrastructure, data, software, and procedures required to remediate incidents to continue to meet objectives are identified, and the change process is initiated upon identification.	Inspected the most current incident response policy and procedures to determine system changes to remediate incidents were required to be identified and executed per the change management process. Informed by Management there were no security incidents reported during the period under review.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Change Management (Continued)			
CC8.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC8.1 (Cont.)	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Creates Baseline Configuration of IT Technology—A baseline configuration of IT and control systems is created and maintained.	Inspected the entity's most current job control policy and procedures, along with the entity's server hardening guidelines adopted by IT Management, to determine a baseline configuration of IT and control systems was created and maintained.	No exceptions noted.
		Provides for Changes Necessary in Emergency Situations—A process is in place for authorizing, designing, testing, approving, and implementing changes necessary in emergency situations (that is, changes that need to be implemented in an urgent timeframe).	Inspected the most current emergency change request policy and procedures to determine a process was in place for the lifecycle management of emergency change requests.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Mitigation**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	Considers Mitigation of Risks of Business Disruption—Risk mitigation activities include the development of planned policies, procedures, communications, and alternative processing solutions to respond to, mitigate, and recover from security events that disrupt business operations. Those policies and procedures include monitoring processes and information and communications to meet the entity's objectives during response, mitigation, and recovery efforts.	Inspected the most current risk register, internal audit checklist, and business continuity and disaster recovery plan to determine the entity considered mitigation of risks of business disruption and had policies and procedures in place to meet entity objectives.	No exceptions noted.
		Considers the Use of Insurance to Mitigate Financial Impact Risks—The risk management activities consider the use of insurance to offset the financial impact of loss events that would otherwise impair the ability of the entity to meet its objectives.	Inspected the most current insurance declarations to determine risk management activities considered the use of insurance to offset the impact of loss events.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	**Risk Mitigation (Continued)**			
CC9.0	**Trust Services Criteria for the Security Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	Establishes Requirements for Vendor and Business Partner Engagements—The entity establishes specific requirements for a vendor and business partner engagement that includes (1) scope of services and product specifications, (2) roles and responsibilities, (3) compliance requirements, and (4) service levels.	Inspected the most current vendor management policy and procedures, along with an executed business associate agreement, to determine the entity established specific requirements for vendor and business partner engagements that included scope of services and specifications, roles and responsibilities, compliance requirements, and service levels.	No exceptions noted.
		Assesses Vendor and Business Partner Risks—The entity assesses, on a periodic basis, the risks that vendors and business partners (and those entities’ vendors and business partners) represent to the achievement of the entity's objectives.	Inspected the most current risk register, an executed business associate agreement, and completed SOC reports of the entity’s subservice organizations to determine vendor and business partner risks were assessed on a periodic basis.	No exceptions noted.
		Assigns Responsibility and Accountability for Managing Vendors and Business Partners—The entity assigns responsibility and accountability for the management of risks associated with vendors and business partners.	Inspected the most current risk register and vendor management policy and procedures to determine the entity assigned responsibility and accountability for the management of risks associated with vendors and business partners.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Mitigation (Continued)			
CC9.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC9.2 (Cont.)	The entity assesses and manages risks associated with vendors and business partners.	Establishes Communication Protocols for Vendors and Business Partners—The entity establishes communication and resolution protocols for service or product issues related to vendors and business partners.	Inspected the most current vendor management policy and procedures, an executed business associate agreement, and the entity's client portal for managing and tracking job orders to determine the entity established communication and resolution protocols for service issues related to vendors and business partners.	No exceptions noted.
		Establishes Exception Handling Procedures from Vendors and Business Partners—The entity establishes exception handling procedures for service or product issues related to vendors and business partners.	Inspected the most current vendor management policy and procedures, an executed business associate agreement, and the entity's client portal for managing and tracking job orders to determine the entity established exception handling procedures for service issues related to vendors and business partners.	No exceptions noted.
		Assesses Vendor and Business Partner Performance—The entity periodically assesses the performance of vendors and business partners.	Inspected the most current risk register, an executed business associate agreement, and completed SOC reports of the entity's subservice organizations to determine the entity periodically assessed the performance of vendors and business partners.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
TSC REF #	Risk Mitigation (Continued)			
CC9.0	Trust Services Criteria for the Security Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
CC9.2 (Cont.)	The entity assesses and manages risks associated with vendors and business partners.	Implements Procedures for Addressing Issues Identified During Vendor and Business Partner Assessments—The entity implements procedures for addressing issues identified with vendor and business partner relationships.	Inspected the most current vendor management policy and procedures, an executed business associate agreement, and the entity's client portal for managing and tracking job orders to determine the entity implemented procedures for addressing issues identified with vendor and business partner relationships.	No exceptions noted.
		Implements Procedures for Terminating Vendor and Business Partner Relationships—The entity implements procedures for terminating vendor and business partner relationships.	Inspected the most current vendor management policy and procedures, along with an executed business associate agreement, to determine the entity implemented procedures for terminating vendor and business partner relationships.	No exceptions noted.

Additional Criteria Related to the Availability Category

	Trust Services Criteria and Points of Focus			
REF	Additional Criteria for Availability			
A1.0	Trust Services Criteria for the Availability Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.	Measures Current Usage—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.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators and system generated usage trending; and inspected the process and Management communications regarding forecasted production equipment expenditures to determine the use of system components was measured to establish a baseline for capacity management and risk of impaired availability due to capacity constraints.	No exceptions noted.
		Forecasts Capacity—The expected average and peak use of system components is forecasted and compared to system capacity and associated tolerances. Forecasting considers capacity in the event of the failure of system components that constrain capacity.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators and system generated usage trending; and inspected the process and Management communications regarding forecasted production equipment expenditures to determine forecasting considered system component utilization to mitigate failure of system components due to capacity.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
REF	Additional Criteria for Availability			
A1.0	Trust Services Criteria for the Availability Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
A1.1 (Cont.)	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.	Makes Changes Based on Forecasts—The system change management process is initiated when forecasted usage exceeds capacity tolerances.	Observed via walkthrough procedures, the network and server monitoring management interface, performance indicators and system generated usage trending; and inspected the process and Management communications regarding forecasted production equipment expenditures to determine forecasted usage was compared to capacity tolerances and any identified system change requests required approval and processing through the change management process.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
REF	Additional Criteria for Availability (Continued)			
A1.0	Trust Services Criteria for the Availability Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Identifies Environmental Threats—As part of the risk assessment process, management identifies environmental threats that could impair the availability of the system, including threats resulting from adverse weather, failure of environmental control systems, electrical discharge, fire, and water.	Inspected the most current risk register and environmental control policy and procedures, along with digital evidence of the entity's video surveillance, fire suppression, monitored security alarm, temperature monitoring, uninterruptible power supply (UPS), and power generator systems to determine Management identified environmental threats that could impair the availability of the system.	No exceptions noted.
		Designs Detection Measures—Detection measures are implemented to identify anomalies that could result from environmental threat events.	Inspected digital evidence of the entity's video surveillance, fire suppression, monitored security alarm, temperature monitoring, UPS, and power generator systems to determine detection measures were implemented to identify anomalies with respect to environmental threat events.	No exceptions noted.
		Implements and Maintains Environmental Protection Mechanisms—Management implements and maintains environmental protection mechanisms to prevent and mitigate against environmental events.	Inspected digital evidence of the entity's video surveillance, fire suppression, monitored security alarm, temperature monitoring, UPS, and power generator systems to determine Management implemented and maintained environmental protection mechanisms to prevent and mitigate against environmental events.	No exceptions noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
REF	Additional Criteria for Availability (Continued)			
A1.0	Trust Services Criteria for the Availability Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
A1.2 (Cont.)	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	<u>Implements Alerts to Analyze Anomalies</u>—Management implements alerts that are communicated to personnel for analysis to identify environmental threat events.	Inspected the most current physical and environmental testing log and conducted corroborative inquiry of IT Management to determine Management implemented alerts for personnel to identify and analyze environmental threat events. Informed by Management there were no environmental threat alerts generated during the period under review.	No exceptions noted.
		<u>Responds to Environmental Threat Events</u>—Procedures are in place for responding to environmental threat events and for evaluating the effectiveness of those policies and procedures on a periodic basis. This includes automatic mitigation systems (for example, uninterruptable power system and generator backup subsystem).	Inspected the most current physical and environmental testing log and conducted corroborative inquiry of IT Management to determine procedures were in place for responding to environmental threat events.	No exceptions noted.
		<u>Communicates and Reviews Detected Environmental Threat Events</u>—Detected environmental threat events are communicated to and reviewed by the individuals responsible for the management of the system, and actions are taken, if necessary.	Inspected the most current physical and environmental testing log and conducted corroborative inquiry of IT Management to determine detected events would be communicated to and reviewed by responsible parties and actions were taken.	No exception noted.

	TRUST SERVICES CRITERIA AND POINTS OF FOCUS			
REF	Additional Criteria for Availability (Continued)			
A1.0	Trust Services Criteria for the Availability Category	Description of Points of Focus	Ascend Audit & Advisory Tests of Points of Focus	Test Results
A1.2 (Cont.)	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	<u>Determines Data Requiring Backup</u>—Data is evaluated to determine whether backup is required.	Inspected the data backup procedures as contained in the most current information security policy procedures and observed via walkthrough procedures, the entity's cloud based backup software, backup job scheduler, and backup job status indicators to determine data was evaluated for backup requirements.	No exceptions noted.
		<u>Performs Data Backup</u>—Procedures are in place for backing up data, monitoring to detect backup failures, and initiating corrective action when such failures occur.	Observed via walkthrough procedures, the entity's cloud based backup software, backup job scheduler, and backup job status indicators to determine procedures were in place for backing up data and monitoring to detect backup failure.	No exceptions noted.
		<u>Addresses Offsite Storage</u>—Backup data is stored in a location at a distance from its principal storage location sufficient that the likelihood of a security or environmental threat event affecting both sets of data is reduced to an appropriate level.	Observed via walkthrough procedures, the entity's cloud based backup software and logical location of completed backup job; and inspected the entity's media use and transit log of backup data to and from an offsite location to determine backup data was stored in an offsite location in a secure manner.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
REF	**Additional Criteria for Availability (Continued)**			
A1.0	**Trust Services Criteria for the Availability Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
A1.2 (Cont.)	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.	Implements Alternate Processing Infrastructure—Measures are implemented for migrating processing to alternate infrastructure in the event normal processing infrastructure becomes unavailable.	Inspected the redundancy policy as contained in the most current information security policy and procedures, along with digital evidence of the entity's disaster recovery processing site, to determine measures were implemented for migrating processing to alternate infrastructure when necessary.	No exceptions noted.

	Trust Services Criteria and Points of Focus			
REF	**Additional Criteria for Availability (Continued)**			
A1.0	**Trust Services Criteria for the Availability Category**	**Description of Points of Focus**	**Ascend Audit & Advisory Tests of Points of Focus**	**Test Results**
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.	Implements Business Continuity Plan Testing—Business continuity plan testing is performed on a periodic basis. The testing includes (1) development of testing scenarios based on threat likelihood and magnitude; (2) consideration of system components from across the entity that can impair the availability; (3) scenarios that consider the potential for the lack of availability of key personnel; and (4) revision of continuity plans and systems based on test results.	Inspected the most current business continuity and disaster recovery plan, along with completed disaster recovery testing results, to determine business continuity testing was performed on a periodic basis.	No exceptions noted.
		Tests Integrity and Completeness of Backup Data—The integrity and completeness of backup information is tested on a periodic basis.	Inspected a completed data restore request, along with completed disaster recovery testing results, to determine the integrity and completeness of backup information was tested on a periodic basis.	No exceptions noted.