SourceOne Output Technologies, Inc.

AT 101 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

February 1, 2017 – January 31, 2018

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

Scott Caldarera
Chief Information Officer
SourceOne Output Technologies, Inc.
711 Bond Avenue
Little Rock, AR 72202

Scope

We have examined the description titled "Description of SourceOne Output Technologies, Inc.'s Marketing, Print, and Fulfillment System throughout the period February 1, 2017 through January 31, 2018" ("the description") and the suitability of the design and operating effectiveness of controls to meet the criteria for the security and availability principles set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids*) (applicable trust services criteria), throughout the period February 1, 2017 through January 31, 2018. The description indicates that certain applicable trust services criteria specified in the description can be achieved only if complementary user-entity controls contemplated in the design of SourceOne Output Technologies, Inc.'s ("SourceOne" or "the Company") controls are suitably designed and operating effectively along with related controls at the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user-entity controls.

SourceOne Output Technologies, Inc.'s Responsibilities

In Section II, the Company has provided an assertion regarding the fair presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the applicable trust services criteria throughout the period February 1, 2017 through January 31, 2018. SourceOne is responsible for (1) preparing the description and assertion; (2) the completeness, accuracy, and method of presentation of both the description and assertion; (3) providing the services covered by the description; (4) specifying the controls that meet the applicable trust services criteria and stating them in the description; and (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria set forth in the Company's assertion and on the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria, based on our examination. We conducted our examination 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, (1) the description is fairly presented based on the description criteria, and (2) the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period February 1, 2017 through January 31, 2018.

Our examination involved performing procedures to obtain evidence about the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of those controls to meet the applicable trust services criteria. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to meet the applicable trust services criteria. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the applicable trust services criteria were met. Our examination also included evaluating the overall presentation of the description. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Inherent Limitations

Because of their nature and inherent limitations, controls at a service organization may not always operate effectively to meet the applicable trust services criteria. Also, the projection to the future of any evaluation of the fairness of the presentation of the description or conclusions about the suitability of the design or operating effectiveness of the controls to meet the applicable trust services criteria is subject to the risks that the system may change or that controls at a service organization may become inadequate or fail.

Opinion

a. The description fairly presents the system that was designed and implemented throughout the period February 1, 2017 through January 31, 2018.

b. The controls stated in the description were suitably designed to provide reasonable assurance that the applicable trust services criteria would be met if the controls operated effectively throughout the period February 1, 2017 through January 31, 2018, and user entities applied the complementary user-entity controls contemplated in the design of SourceOne's controls throughout the period February 1, 2017 through January 31, 2018.

c. The controls tested, which together with the complementary user-entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the applicable trust services criteria were met, operated effectively throughout the period February 1, 2017 through January 31, 2018.

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.

Restricted Use

This report and the description of tests of controls and results thereof are intended solely for the information and use of the Company, user entities of the Company's system throughout the period February 1, 2017 through January 31, 2018, 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

February 20, 2018

II. Information Provided by SourceOne Output Technologies, Inc.

MANAGEMENT ASSERTION LETTER

We have prepared the description of SourceOne Output Technologies, Inc.'s Marketing, Print, and Fulfillment System ("the description") throughout the period February 1, 2017 through January 31, 2018, ("the description") based on the criteria in items (a)(i) – (ii) below, which are the criteria for a description of a service organization's system in Paragraphs 1.34-.35 of the AICPA Guide *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy* (the description criteria). The description is intended to provide users with information about the system, particularly system controls intended to meet the criteria for the security and availability principles set forth in TSP Section 100, *Trust Services Principles, Criteria, and Illustrations for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Technical Practice Aids)* (applicable trust services criteria). We confirm, to the best of our knowledge and belief, that:

a. The description fairly presents the system throughout the period February 1, 2017 through January 31, 2018, based on the following 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 principle 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 specified period to meet the applicable trust services criteria.

c. The controls stated in the description operated effectively throughout the specified period to meet the applicable trust services criteria.

By: /S/ Scott Caldarera

Scott Caldarera
Chief Information Officer

February 20, 2018

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 with 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.

System Description

The 2017 SOC 2 examination covers SourceOne Output Technology's Technology 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.

Infrastructure

The SourceOne Output Technology's Information Technology (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 camera, including the external grounds.

The accompanying SOC 2 examination report covers the IT infrastructure supporting the following technology solutions, which are developed and managed by SourceOne Output Technology:

• SourceOne Document / Statement / Marketing Fulfillment Systems & Services

Infrastructure Services is presently responsible for supporting approximately 2 servers supporting the in-scope technology solutions. These servers are summarized below by operating system and the 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 Output Technology IT Environment includes:

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

The SourceOne Output Technology's IT Environment described herein does not include application software supporting the technology solutions provided by SourceOne Output Technology to individual clients or SourceOne Output Technology business unit applications.

People

IT personnel provide the following core support services over the SourceOne Output Technology's IT Environment components above:

- 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 three functional areas: Network Services, Development, and Support. Below is a brief description of each of these functional areas:

- **Network Management Services:** 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.

- **Development:** The team overseas the new product developments, client customizations, and new releases and updates for client software.
- **Support:** The team deals with maintenance, repairs, and upgrades attending to client support.

Procedures

SourceOne Output Technology 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 the MSSQL 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 also responsible for the overall availability of data, including system backups, monitoring of data processing and file transmissions as well as identifying and resolving problems.

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's ethics policy may be subject to disciplinary action, up to and including termination of employment.

Commitment to Competence

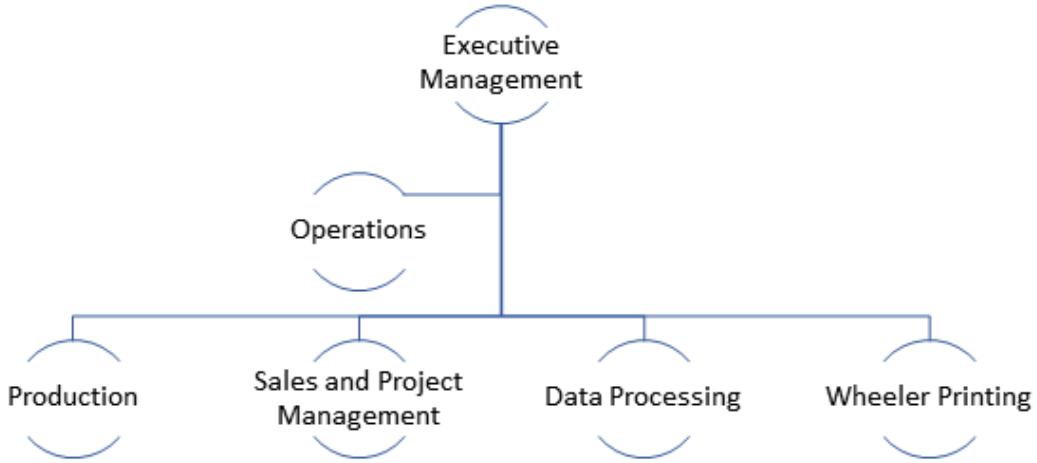
The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company determines the knowledge and skills needed to perform job duties and responsibilities and hires for that skill 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's 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.

Human Resources Policies and Procedures

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.

Standard Operating Controls

SourceOne's 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.

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's management performs periodic audits of procedures and holds scheduled compliance meetings with staff to review current and new procedures.

Risk Assessment

SourceOne's 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 departments/divisions 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.

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 PRINCIPLE

REF	Common Criteria Related to Organization and Management			
CC1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC1.1	The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security and availability.	SourceOne has a high-level business unit organizational chart.	Inspected the most current organizational chart to determine it was in place and current.	No exceptions noted.
		SourceOne has written job descriptions specifying the responsibilities, academic, and professional requirements for key job positions.	Inspected the management job descriptions for positions charged with security and governance of the system to determine they specified the responsibilities, academic, and professional requirements for key job positions.	No exceptions noted.
		Job descriptions exists for personnel with elevated access to the system.	Inspected the IT Security job description to determine job descriptions were in place for personnel with elevated access to the system.	No exceptions noted.
		SourceOne roles and responsibilities are defined and written in job descriptions that are controlled documents and available to all staff including managers and supervisors.	Inspected a screenshot of the location of written job descriptions to determine they were controlled documents and were available to all staff.	No exceptions noted.
		SourceOne's Human Resources (HR) Department reviews job descriptions periodically or as needed in events of job duty changes.	Inspected the revision history of IT Security job description to determine HR reviewed job descriptions on an as needed basis.	No exceptions noted.

REF	Common Criteria Related to Organization and Management (Continued)			
CC1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC1.2	Responsibility and accountability for designing, developing, implementing, operating, maintaining, monitoring, and approving the entity's system controls and other risk mitigation strategies are assigned to individuals within the entity with authority to ensure policies and other system requirements are effectively promulgated and implemented to meet the entity's commitments and system requirements as they relate to security and availability.	The responsibility and accountability for the maintenance and enforcement of the Company's Information Security Policy is assigned to the Chief Technology Officer (CTO). SourceOne's Human Resources (HR) Department reviews job descriptions periodically or as needed in events of job duty changes.	Inspected the most current Information Security Policy and the CIO job description to determine the responsibility and accountability for the maintenance and enforcement of the Information Security Policy was assigned to the CIO. Inspected the revision history of the IT Security job description to determine HR reviewed job descriptions periodically or on an as needed basis.	No exceptions noted. No exceptions noted.

REF	Common Criteria Related to Organization and Management (Continued)			
CC1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC1.3	The entity has established procedures to evaluate the competency of personnel responsible for designing, developing, implementing, operating, maintaining, and monitoring the system affecting security and availability and provides resources necessary for personnel to fulfill their responsibilities.	SourceOne has written job descriptions specifying the responsibilities, academic, and professional requirements for key job positions.	For a sample of key positions, inspected written job descriptions to determine the job descriptions included responsibilities, academic, and professional requirements.	No exceptions noted.
		SourceOne monitors and keeps track of compliance and training records for all its employees.	For the selection of active employees, inspected training participation records to determine SourceOne monitored and tracked compliance and training for all its employees.	No exceptions noted.
		SourceOne's HR Department has established training for all new and existing staff at the time of hire and annually.	Inspected a screenshot of available training acknowledgements to determine the Company had established training for existing staff. *Informed by management that no new hires were reported for the audit period.*	No exceptions noted.

REF	Common Criteria Related to Organization and Management (Continued)			
CC1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC1.4	The entity has established workforce conduct standards, implemented workforce candidate background screening procedures, and conducts enforcement procedures to enable it to meet its commitments and system requirements as they relate to security and availability.	SourceOne employees are required to follow Company policy regarding code of conduct. A formal disciplinary policy is in place.	Inspected a completed disciplinary form to determine that employees were required to follow Company policy regarding code of conduct.	No exceptions noted.
		Personnel are required to read and accept the code of conduct and the statement of confidentiality and privacy practices upon their hire and to formally re-affirm them annually thereafter.	Inspected the Code of Conduct, Confidentiality and Privacy practices, and the Employee Handbook to determine policies were available. *Informed by Management that no new hires were reported for the audit period.*	No exceptions noted.
		Personnel must pass a criminal background check before they may be hired by the Company or third-party vendors hired by the Company.	Inspected the third-party service contract to determine it was in place. *Informed by Management that no new hires were reported for the audit period.*	No exceptions noted.

REF	Common Criteria Related to Communication			
CC2.0	Criteria	Control	Test Performed	Test Results
CC2.1	Information regarding the design and operation of the system and its boundaries has been prepared and communicated to authorized internal and external users of the system to permit users to understand their role in the system and the results of system operation.	SourceOne posts a description of its system, system boundaries, and system processes that includes infrastructure, software, people, procedures, and is available on a shared network location for internal users.	Inspected the most current system description and a screenshot of its location to determine: it was in place; addressed system boundaries, and system processes that included infrastructure, software, people, and procedures; and was available on a shared network location.	No exceptions noted.

REF	Common Criteria Related to Communication (Continued)			
CC2.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC2.2	The entity's security and availability commitments are communicated to external users, as appropriate, and those commitments and the associated system requirements are communicated to internal users to enable them to carry out their responsibilities.	Policy and procedures documents for significant processes are available on SourceOne's file share. SourceOne requires annual security training of its employees. New employees are required to acknowledge all SourceOne policies as part of the orientation process.	Inspected the location of the Company's in-scope policies to determine policies and procedures were made available on SourceOne's file share. The annual security training program was implemented during the period. Inspected in scope policy signoff requirements. *Informed by Management that no new hires were reported for the audit period.*	No exceptions noted. No testing performed. No testing performed.

REF	Common Criteria Related to Communication (Continued)			
CC2.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC2.3	The responsibilities of internal and external users and others whose roles affect system operation are communicated to those parties.	Policy and procedures documents for significant processes are available on a shared network for all employee access. All employees are required to acknowledge all SourceOne policies including a code of conduct and confidentiality statement, as part of the orientation process.	Inspected the network location to determine it was shared and maintained all relevant policies and procedures. Inspected the Code of Conduct, Confidentiality and Privacy practices, and the Employee Handbook to determine policies required sign-off. *Informed by Management that no new hires were reported for the audit period.*	No exceptions noted. No exceptions noted.

REF	Common Criteria Related to Communication (Continued)			
CC2.0	Criteria	Control	Test Performed	Test Results
CC2.4	Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security and availability of the system, is provided to personnel to carry out their responsibilities.	Policy and procedures documents for significant processes are available on a shared network for all employee access.	Inspected the network location to determine it was shared and maintained all relevant policies and procedures.	No exceptions noted.
CC2.5	Internal and external users have been provided with information on how to report security and availability failures, incidents, concerns, and other complaints to appropriate personnel.	The SourceOne Incident Response policy provides guidance to employees for how to identify and report possible security breaches.	The Incident response plan was implemented during the audit period under review and maintained defined protocols and procedures for handling incidents.	No testing performed.

REF	Common Criteria Related to Communication (Continued)			
CC2.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC2.6	System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security and availability are communicated to those users in a timely manner.	SourceOne has a change control procedure in the Information Security Policy. Communications regarding changes and outages are to be reported by email and must be approved.	Inspected the most current change control procedures to determine they provided the communication protocol for changes and outages to be reported by email after approved.	No exceptions noted.
		All system changes are communicated to all employees via email once approved.	Inspected a sample of system change notifications to determine all system changes were emailed to staff once approved.	No exceptions noted.
		Roles and responsibility changes are documented in the shared network drive which is controlled and available for all employees.	Inspected a screenshot of the network location to determine roles and responsibility changes were documented, controlled and available to all employees.	No exceptions noted.

REF	Common Criteria Related to Risk Management and Design and Implementation of Controls			
CC3.0	Criteria	Control	Test Performed	Test Results
CC3.1	The entity (1) identifies potential threats that could impair system security and availability commitments and system requirements (including threats arising from the use of vendors and other third parties providing goods and services, as well as threats arising from customer personnel and others with access to the system), (2) analyzes the significance of risks associated with the identified threats, (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods or services, as well as their activities, and other mitigation strategies), (4) identifies and assesses changes (for example, environmental, regulatory, and technological changes and results of the assessment and monitoring of controls) that could significantly affect the system of internal control, and (5) reassesses, and revises, as necessary, risk assessments and mitigation strategies based on the identified changes.	The Company maintains records of IT assets. The records are updated as part of the change management process. SourceOne Executive Team are responsible for the formal risk management process. The risk management process includes evaluation, rating and management reviews. SourceOne utilizes network monitoring systems to capture key system information.	Inspected the current IT asset inventory list to determine the Company maintained records of IT assets as part of the change management process. Inspected the most current risk monitoring checklist and a sample of Privacy and Security Council Meeting Minutes to determine Senior Management were responsible for the risk management process which included evaluation, rating and management reviews. Inspected screenshots of the location of key system information to determine system information was captured by automated checks and logging.	No exceptions noted. No exceptions noted. No exceptions noted.

REF	Common Criteria Related to Risk Management and Design and Implementation of Controls (Continued)			
CC3.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC3.2	The entity designs, develops, implements, and operates controls, including policies and procedures, to implement its risk mitigation strategy; reassesses the suitability of the design and implementation of control activities based on the operation and monitoring of those activities; and updates the controls, as necessary.	SourceOne has a written Security Policy, which addresses IT and physical security, in place, which is reviewed throughout the year by the Privacy and Security Council.	Inspected the revision history of the Security Policies and Management Plan to determine the Company had a written policy, that it addressed IT and physical security, and was reviewed at least once during the past twelve (12) months.	No exceptions noted.
		SourceOne Executive Team meets monthly to review and/or suggest policy changes. Any relevant changes are communicated to authorized users.	Inspected a sample of completed monthly meeting minutes to determine meetings were held to review and/or suggest policy changes.	No exceptions noted.

REF	Common Criteria Related to the Monitoring of Controls			
CC4.0	Criteria	Control	Test Performed	Test Results
CC4.1	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	The enterprise anti-virus system has been configured to provide alerts to administrators when the system detects malicious code. Definition files are updated throughout the day.	Inspected a sample of system generated alerts to determine the enterprise anti-virus system had been configured to provide alerts to administrators when the system detects malicious code.	No exceptions noted.
			Inspected a screenshot of the anti-virus polling configuration to determine the definition files were updated throughout the day.	No exceptions noted.
		An enterprise monitoring application is utilized to monitor critical server capacity and performance parameters. Alerts are sent to administrators in the event a system is operating outside of pre-defined parameters.	Inspected a screenshot of the system monitoring reports to determine an enterprise monitoring application was utilized to monitor critical server capacity and performance parameters.	No exceptions noted.
			Inspected a sample of system generated alerts to determine alerts were sent to administrators in the event a system was operating outside of pre-defined parameters.	No exceptions noted.

REF	Common Criteria Related to the Monitoring of Controls (Continued)			
CC4.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC4.1 (Cont.)	The design and operating effectiveness of controls are periodically evaluated against the entity's commitments and system requirements as they relate to security and availability and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.	An intrusion detection system (IDS) is utilized and configured to send alerts to the Security Engineer for events such as: • Daily intrusion detection system (IDS) or intrusion prevention system (IPS) attacks • Critical IDS or IPS alerts • Servers not reporting • Firewall configuration changes Reports are logged and reviewed by the Systems Administrator.	Inspected a screenshot of the IDS management console to determine an IDS was utilized and configured to send alerts to the Security Engineer for the following events: • Daily intrusion detection system (IDS) or intrusion prevention system (IPS) attacks • Critical IDS or IPS alerts • Servers not reporting • Firewall configuration changes Inspected a screenshot of report logs to determine reports were logged and reviewed by the Systems Administrator.	No exceptions noted. No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.1	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	When deploying a new server, a hardening checklist is required to be followed.	Inspected the New Server Setup Checklist to determine that when deploying a new server, a hardening checklist was required to be followed.	No exceptions noted.
		SourceOne utilizes role based security to restrict access to confidential data throughout the production workflow based on the staff member's job responsibilities.	Inspected the Active Directory Security Groups to determine SourceOne utilized role based security to restrict access to confidential data based on the staff member's job responsibilities.	No exceptions noted.
		The roles are enforced by the Active Directory (AD) system and are applied to directories used to store or process client files for which services are to be performed.	Inspected screenshots of the AD, Client Services Security Group, its properties, and membership to determine roles were enforced and applied by the AD for client files for which services were to be performed.	No exceptions noted.
		SourceOne maintains a data classification policy. All new data that falls outside of standard transfers is identified and classified according to its sensitivity.	Informed by management that the policy was implemented during the audit period under review.	No testing performed.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.1 (Cont.)	Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of authorized internal and external users; (2) restriction of authorized internal and external user access to system components, or portions thereof, authorized by management, including hardware, data, software, mobile devices, output, and offline elements; and (3) prevention and detection of unauthorized access to meet the entity's commitments and system requirements as they relate to security and availability.	External access by employees is permitted only through a two-factor (for example, a swipe card and a password) encrypted virtual private network (VPN) connection.	Inspected a screenshot of the VPN encryption configuration to determine external access by employees was permitted only through a two-factor, encrypted VPN connection.	No exceptions noted.
		SourceOne restricts remote access to VPN connections only, which is authenticated by an Active Directory (AD) security group.	Inspected a screenshot of the AD VPN Security Group and its membership to determine SourceOne restricted remote access to VPN connections only; and authenticated remote users by an AD security group.	No exceptions noted.
		SourceOne assets are assigned to individual owners or shared groups in the production facility. There are no shared account usages on any assets with access to confidential data. All access change requests are submitted to HR and the Help Desk.	Inspected a sample of employee change tickets to determine all access change requests were submitted to HR and the Help Desk.	No exceptions noted.
		External points of connectivity are protected by a firewall appliance.	Inspected screenshots of the firewall management interface, firewall ingress and egress rules, and the network topology to determine external points of connectivity were protected by a firewall appliance.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.2	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	SourceOne utilizes new user tickets to document the new account provisioning and authorization process. New user access requests must be approved by an authorized individual.	Inspected via walkthrough procedures that SourceOne maintained a ticketing software application for new authorization and provisioning processes. *Informed by management that no new hires were reported for the audit period.*	No exceptions noted.
		SourceOne has a process for new hires and terminations, where a ticket is created and assigned to IT for resolution of the account change or termination. Access is terminated in a timely manner according to the nature of the request.	Inspected via walkthrough procedures that SourceOne maintained a ticketing software application for new authorization and provisioning processes.	No exceptions noted.
		All SourceOne Domain Account passwords expire every 90 days.	Inspected screenshots of the SourceOne Domain Account Password policies to determine passwords expired every 90 days.	No exceptions noted.
		All access requests must be submitted by Management and approved by Senior IT Management prior to activation, reactivation or termination.	Inspected the HR new hire process via walkthrough procedures to determined that ticketing software was utilized to activate, terminate, or reissue access requests *Informed by management that no terminated staff had network access rights during the audit period.*	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.2 (Cont.)	New internal and external users, whose access is administered by the entity, are registered and authorized prior to being issued system credentials and granted the ability to access the system to meet the entity's commitments and system requirements as they relate to security and availability. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	SourceOne policies prohibit the use of shared accounts unless the account used does not access confidential and private data.	Inspected the most current SourceOne Security Policies and Management Plan to determine the policies prohibited the use of shared accounts.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.3	Internal and external users are identified and authenticated when accessing the system components (for example, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security and availability.	Shared sign-on is restricted to production print job runs only. There is no shared sign-on access to the corporate network.	Inspected the Active Directory, production print job properties and its membership to determine shared sign-on was restricted to production print job runs only and there was no shared sign-on access to the corporate network.	No exceptions noted.
		SourceOne utilizes two-factor authentication for its encrypted VPN access.	Inspected a screenshot of the VPN authentication configuration to determine the Company utilized two-factor authentication for its encrypted VPN access.	No exceptions noted.
		Unique user identification names and passwords are required to authenticate all users to the corporate network. Password parameters consist of the following: • Passwords are at least eight (8) characters • Passwords expire every thirty (90) days • Password lockout after three (3) failed attempts • Operating system enforces password complexity	Inspected a screenshot of the domain password settings to determine unique user identification names and passwords were required to authenticate all users and password parameters consisted of the following: • Passwords were at least eight (8) characters • Passwords expired every thirty (90) days • Password lockout after three (3) failed attempts • Operating system enforced password complexity	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.4	Access to data, software, functions, and other IT resources is authorized and is modified or removed based on roles, responsibilities, or the system design and changes to meet the entity's commitments and system requirements as they relate to security and availability.	SourceOne utilizes tickets to document the new account provisioning and authorization process. New user access requests must be approved by an authorized individual.	Inspected via walkthrough procedures that SourceOne maintained a ticketing software application for new authorization and provisioning processes. *Informed by management that no new hires were reported for the audit period.*	No exceptions noted.
		SourceOne has a process for new hires and terminations, where a ticket is created and assigned to IT for resolution of the account change or termination.	Inspected the HR new hire process via walkthrough procedures to determined that ticketing software was in utilized to activate, terminate, or reissue access requests *Informed by management that no staff were added. Informed by management that no terminated staff had network access rights during the audit period.*	No exceptions noted.
		SourceOne security and data access is role based. Only certain uses have remote access to the data and a two-factor authentication is required for all remote access.	Inspected the Active Directory Security Groups and its associated membership to determine SourceOne security and data access was role based.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	Criteria	Control	Test Performed	Test Results
CC5.5	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	Physical access to the IT resources, servers, backup media, and related hardware, such as firewalls and routers, is restricted to authorized individuals by keypad systems.	Observed via walk-through procedures and inspected a screenshot of the keypad system user listing to determine physical access to the data centers was restricted to authorized personnel by card key systems.	No exceptions noted.
		Video surveillance systems are in place to monitor entrances to the facility and critical internal areas.	Observed via walkthrough procedures, the video surveillance systems to determine they were in place and operational.	No exceptions noted.
		Visitors must be signed in by an employee, before a single-day visitor badge that identifies them as an authorized visitor, can be issued.	Observed via onsite inspection, the visitor intake process to determine visitors were required to sign-in and display a visitor access badge.	No exceptions noted.
		All visitors must be escorted by a Company employee when visiting facilities where sensitive system and system components are maintained and operated.	Observed via onsite inspection, the visitor intake process to determine all visitors were escorted by an employee when visiting facilities where sensitive system and components were maintained and operated.	No exceptions noted.
		Access to sensitive areas are requested and approved by the Management team responsible for the area.	Inspected password file for server room access to determine Management approved access to sensitive areas.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.5 (Cont.)	Physical access to facilities housing the system (for example, data centers, backup media storage, and other sensitive locations, as well as sensitive system components within those locations) is restricted to authorized personnel to meet the entity's commitments and system requirements as they relate to security and availability.	All visitors must sign in at the reception desk and are escorted throughout the duration of their visit.	Observed and digitally recorded the visitor sign in process to determine all visitors were required to sign in at the reception desk and were escorted throughout the duration of their visit.	No exceptions noted.
		Access to secured areas such as server rooms are very limited. Authorized non-employees, such as contractors and vendors, must be escorted at all times.	Inspected the access control file for limiting unescorted access to secured areas.	No exceptions noted.
		Management changes the access control PIN code at the time of employee exit.	For the population of terminated employees, inspected completed building access/security code request forms to determine Management changed access control PIN codes at time of employee exit.	No exceptions noted.
		SourceOne Security policies and best practices states no sharing of access codes or tailgating allowed.	Inspected the most current Security policies to determine card code sharing and tailgating was prohibited.	No exceptions noted.
		SourceOne utilizes a man trap for access to its production operations facility.	Observed via walk-through procedures, facility access to determine a man trap was utilized for access to its production operations facility.	No exceptions noted.
		SourceOne production department requires secured keypad access at all ingress/egress points.	Observed via walk-through procedures, facility access to determine facilities were only accessible via security access PIN codes.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.6	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	SourceOne restricts remote access to VPN connections which is authenticated by an Active Directory (AD) security group.	Inspected a screenshot of the AD VPN Security Group and its membership to determine SourceOne restricted remote access to VPN connections only and authenticated by an AD security group.	No exceptions noted.
		Firewall and VPN configurations limit the time that a session can be idle.	Inspected screenshots of the firewall and VPN timeout settings to determine firewall and VPN configurations limited the time that a session could be idle.	No exceptions noted.
		SourceOne uses firewalls to prevent unauthorized access. All traffic to external points must pass through the firewalls.	Inspected a screenshot of the firewall management interface and a screenshot of the network topology to determine SourceOne used firewalls to prevent unauthorized access and all traffic to external points must pass through the firewalls.	No exceptions noted.
		All firewalls are configured, hardened, and upgraded based on best practices and industry standards.	Inspected screenshots of the firewall high availability configuration and access rules to determine firewalls were configured, hardened, and upgraded based on best practices and industry standards.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	Criteria	Control	Test Performed	Test Results
CC5.6 (Cont.)	Logical access security measures have been implemented to protect against security and availability threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.	Firewall rules limit access and the types of activities to external connections based on business requirements and industry standards.	Inspected a screenshot of the firewall access rules to determine firewall rules limited access and types of activities to external connections based on business requirements and industry standards.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	Criteria	Control	Test Performed	Test Results
CC5.7	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	SourceOne restricts remote access to VPN connections which is authenticated by the firewall.	Inspected a screenshot of the VPN authentication to determine the Company restricted remote access to VPN connections which was authenticated by the firewall.	No exceptions noted.
		SourceOne uses a firewall to prevent unauthorized access. All traffic to external points must pass through the firewall.	Inspected a screenshot of the firewall management interface and a screenshot of the network topology to determine SourceOne used a firewall to prevent unauthorized access and all traffic to external points must pass through the firewall.	No exceptions noted.
		Firewall and VPN configurations limit the time that a session can be idle.	Inspected screenshots of the firewall and VPN timeout settings to determine firewall and VPN configurations limited the time that a session could be idle.	No exceptions noted.
		Unencrypted transmission of confidential data outside of SourceOne's network is against policy and prohibited. SourceOne SPAM and content filtering systems are used to scan data for malicious content.	Inspected the most current Information Security Policy to determine unencrypted transmission of confidential data outside of SourceOne's network was against policy and prohibited.	No exceptions noted.
			Inspected screenshots of the anti-virus interface to determine a SPAM and content filtering system was utilized to scan data for malicious content.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.7 (Cont.)	The transmission, movement, and removal of information is restricted to authorized internal and external users and processes and is protected during transmission, movement, or removal, enabling the entity to meet its commitments and system requirements as they relate to security and availability.	SourceOne backup data are encrypted.	Inspected a screenshot of the backup system data encryption settings to determine SourceOne backup data was encrypted.	No exceptions noted.
		SourceOne workstations and laptop hard drives are fully encrypted. Access to removable media is limited.	Inspected a screenshot of local workstation configuration to determine that third party encryption software was utilized for workstation encryption.	No exceptions noted.
		Only SourceOne IT Operations is authorized to access removable media and backup tapes.	Inspected access controls for physical access to removable media to determine only IT Operations was authorized to access removable media and backup tapes.	No exceptions noted.

REF	Common Criteria Related to Logical and Physical Access Controls (Continued)			
CC5.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
CC5.8	Controls have been implemented to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's commitments and system requirements as they relate to security and availability.	SourceOne uses anti-virus software on Windows-based systems to protect against viruses, malicious code, and unauthorized software. The software is configured for automatic updates to all covered systems.	Inspected screenshots of the anti-virus software management interface to determine that SourceOne used anti-virus software on Windows-based systems to protect against viruses, malicious code, and unauthorized software; and the software was configured for automatic updates to all covered systems.	No exceptions noted.
		SourceOne anti-virus is configured to receive updates daily and as updates become available.	Inspected a screenshot of the anti-virus polling configuration to determine SourceOne anti-virus was configured to receive updates daily and as updates became available.	No exceptions noted.
			Inspected a sample of system generated alerts to determine the anti-virus system sent daily notifications.	No exceptions noted.
		SourceOne Security policies prohibit application installation without prior authorization from IT.	Inspected the Information Security policy to determine that installation of third party software was addressed.	No exceptions noted.

REF	Common Criteria Related to System Operations			
CC6.0	Criteria	Control	Test Performed	Test Results
CC6.1	Vulnerabilities of system components to security and availability breaches and incidents due to malicious acts, natural disasters, or errors are identified, monitored, and evaluated, and countermeasures are designed, implemented, and operated to compensate for known and newly identified vulnerabilities to meet the entity's commitments and system requirements as they relate to security and availability.	Logging and monitoring software is used to collect data from system infrastructure components and endpoint systems and used to monitor system performance, potential security threats and vulnerabilities. This software submits automated notifications to IT Operations.	Inspected a screenshot of the logging and monitoring software management console to determine it was in place and used to collect data from the system infrastructure and endpoints and used to monitor system performance, potential security threats and vulnerabilities.	No exceptions noted.
		Weekly full-system and daily incremental backups are performed using an automated system.	Inspected screenshots of the backup application schedules to determine weekly full-system and daily incremental backups were performed using an automated system.	No exceptions noted.
		SourceOne performs daily and weekly backups using an automated backup and restore system.	Inspected screenshots of the backup and restore schedules to determine SourceOne performed daily and weekly backups using an automated backup and restore system.	No exceptions noted.

REF	Common Criteria Related to System Operations (Continued)			
CC6.0	Criteria	Control	Test Performed	Test Results
CC6.2	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	Security incidents are reported to IT Operations. A help desk ticket is created to track the incident through to resolution.	The Incident response plan was implemented during the audit period under review and maintained defined protocols and procedures for handling incidents. *Informed by management that no incidents were reported during the period.*	No testing performed.
		SourceOne has an established security incident response plan that details how to respond to security or other incidences.	Inspected the most current Incident Response policy to determine it was in place and detailed how to respond to security or other incidences.	No exceptions noted.
		Change management requests are opened for security incident events that require permanent fixes.	The Incident response plan was implemented during the audit period under review and maintained defined protocols and procedures for handling incidents. *Informed by management that no incidents were reported during the period.*	No testing performed.
		SourceOne's policies include probation, suspension, and termination as potential sanctions for employee misconduct.	Inspected the most current Employee Handbook to determine SourceOne policies included probation, suspension, and termination as potential sanctions for employee misconduct.	No exceptions noted.

REF	Common Criteria Related to System Operations (Continued)			
CC6.0	Criteria	Control	Test Performed	Test Results
CC6.2 (Cont.)	Security and availability incidents, including logical and physical security breaches, failures, and identified vulnerabilities, are identified and reported to appropriate personnel and acted on in accordance with established incident response procedures to meet the entity's commitments and system requirements.	SourceOne Security has defined protocols and procedures documented in the SourceOne Incident Response plan.	The Incident response plan was implemented during the audit period under review and maintained defined protocols and procedures for handling incidents.	No testing performed.
		All security incidents are documented and reviewed at weekly Operations Group meeting.	Inspected calendar schedules to determine weekly meetings were held. *Informed by management that no incidents were reported during the period.*	No exceptions noted.
		SourceOne documents all security incidents in its ticket system. All staff are informed immediately after an incident has been reported and throughout the remediation process.	Inspected the ticket system to determine SourceOne had the ability to document security incidents. *Informed by management that no incidents were reported during the period.*	No exceptions noted.

REF	Common Criteria Related to Change Management			
CC7.0	Criteria	Control	Test Performed	Test Results
CC7.1	The entity's commitments and system requirements, as they relate to security and availability are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.	System change requests are evaluated to determine the potential effect of the change or security and availability commitments and requirements throughout the change management process.	Inspected a completed change communication to determine that change requests were evaluated to determine the potential effect of the change or security and availability commitments and requirements throughout the change management process.	No exceptions noted.
CC7.2	Infrastructure, data, software, and policies and procedures are updated as necessary to remain consistent with the entity's commitments and system requirements as they relate to security and availability.	Servers are reviewed and patched as necessary by IT Operations according to the criticality of the server system.	Inspected screenshots of completed patch updates to determine backup and domain controller servers were reviewed and patched as necessary by IT Operations.	No exceptions noted.
		Workstation patch management is managed by IT Operations to ensure workstations are updated with the latest patches.	Inspected a sample of update history via physical walkthrough procedures to determine that workstation patch management was managed by IT Operations to ensure workstations were updated with the latest patches.	No exceptions noted.
		All security incidents are documented and reviewed. All change management requests will be documented in the Company ticketing system.	Informed by management that no incidents were reported during the period under review.	No testing performed.

REF	Common Criteria Related to Change Management (Continued)			
CC6.0	Criteria	Control	Test Performed	Test Results
CC7.3	Change management processes are initiated when deficiencies in the design or operating effectiveness of controls are identified during system operation and are monitored to meet the entity's commitments and system requirements as they relate to security and availability.	For high severity incidents, a root cause analysis is prepared and reviewed by Operations Management and any resultant remediation is incorporated into the change management process.	Inspected the communication history of a high severity incident to determine a root cause analysis was prepared and reviewed by Operations Management, as part of the change management process.	No exceptions noted.

REF	Common Criteria Related to Change Management (Continued)			
CC7.0	Criteria	Control	Test Performed	Test Results
CC7.4	Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security and availability commitments and system requirements.	SourceOne has documented change control procedures that are tracked through a ticket system that includes appropriate approval, necessary communications, proper version control, and application documentation.	Inspected a completed change request ticket to determine the Company followed change control procedures and tracked changes through a ticket system.	No exceptions noted.
		Separate environments are used for development, testing, and production. Developers do not have the ability to make changes to software in testing or production.	Observed via walkthrough procedures and inspected the architecture of the software development environments to determine development, test, and production environments were logically separated; and developers did not have the ability to make changes to test and production environments.	No exceptions noted.
		SourceOne has emergency change control procedures that handle emergency changes made to rectify major problems outside the normal change process. Procedures include an appropriate approval process prior to change and documentation after the change has been implemented.	Inspected the most current change control procedures to determine SourceOne had emergency change procedures in place to rectify major problems outside the normal change process; and they included proper approvals and documentation prior to and after change implementations.	No exceptions noted.
		Post implementation procedures that are designed to verify the operation of system changes are performed after the implementation, for other than minor changes, and results are shared with users and customers as required to meet commitments and requirements.	Inspected a completed change request ticket to determine post implementation procedures were performed to verify the operation of changes; and results were shared with stakeholders.	No exceptions noted.

ADDITIONAL CRITERIA RELATED TO THE AVAILABILITY PRINCIPLE

REF	Criteria Related to the Availability Principle			
A1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
A1.1	Current processing capacity and usage are maintained, monitored, and evaluated to manage capacity demand and to enable the implementation of additional capacity to help meet the entity's availability commitments and system requirements.	SourceOne performs network capacity planning by using a network monitoring system which monitors CPU utilization, memory, data, links and network traffic.	Inspected a screenshot of the network monitoring dashboard and conducted corroborative inquiry of IT Management to determine SourceOne performed network capacity planning by utilizing the network monitoring application's trending information.	No exceptions noted.
A1.2	Environmental protections, software, data backup processes, and recovery infrastructure are authorized, designed, developed, implemented, operated, approved, maintained, and monitored to meet the entity's availability commitments and system requirements.	SourceOne data is backed up daily and weekly.	Inspected screenshots of daily and weekly backup schedules to determine SourceOne data was backed up daily and weekly.	No exceptions noted.
		SourceOne has multiple controls in place to protect the sever room and its data backup against environmental incidents.	Observed via walkthrough procedures and digitally recorded evidence to determine SourceOne had multiple environmental protection controls in place and functional, for the server room and its data backup.	No exceptions noted.
		SourceOne has a documented disaster recovery plan that is reviewed and tested annually.	Inspected the most current IT Disaster Recovery plan to determine SourceOne had a disaster recovery plan in place; and it was reviewed and tested at least once during the past twelve months.	No exceptions noted.

REF	Criteria Related to the Availability Principle (Continued)			
A1.0	**Criteria**	**Control**	**Test Performed**	**Test Results**
A1.3	Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.	SourceOne has a documented disaster recovery plan that is reviewed and tested annually.	Inspected the most current IT Disaster Recovery Plan and a sample of disaster recovery test results to determine SourceOne had a disaster recovery plan in place; and it was reviewed and tested at least once during the past twelve months.	No exceptions noted.