SOURCEONE OUTPUT TECHNOLOGIES

SSAE 16 SOC 1 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

November 1, 2016 to January 31, 2017

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

TABLE OF CONTENTS

I. Independent Service Auditor's Report ____ *3*

Independent Service Auditor's Report ____ **4**

II. Information Provided by SourceOne Output Technologies ____ *7*

Description of Relevant Controls Provided by SourceOne Output Technologies ____ **8**

Management Assertions Letter ____ 8
Company Overview ____ 10
SourceOne Products and Services Overview ____ 10

Relevant Aspects of the Control Environment, Risk Assessment, Monitoring, Information Systems and Communication ____ **11**

Control Environment ____ 11
Risk Assessment ____ 14
Monitoring ____ 15
Information Systems ____ 15
Communication ____ 19
User Control Considerations ____ 20

III. Information Provided by Ascend Audit & Advisory ____ *21*

Control Objectives, Related Controls, and Tests of Operating Effectiveness ____ **22**

Control Objective 1 – Organization and Administration ____ 22
Control Objective 2 – Information Security: Logical Access ____ 24
Control Objective 3 – Information Security: Physical Access ____ 26
Control Objective 4 – Information Security: Environmental Controls ____ 27
Control Objective 5 – Computer Operations ____ 28
Control Objective 6 – Data Transmission ____ 30
Control Objective 7 – Backup and Data Recovery ____ 31
Control Objective 8 – Disaster Recovery Preparedness ____ 33
Control Objective 9 – Order Processing, Fulfillment and Shipping ____ 34
Control Objective 10 – Inventory Audit ____ 36

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 Operations Officer
SourceOne Output Technologies
711 Bond Avenue
Little Rock, AR 72202

Scope

We have examined SourceOne Output Technologies' (SourceOne or the Company) description of its information technology, print and fulfillment system throughout the period November 1, 2016 to January 31, 2017 and the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description. The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls contemplated in the design of the Company's 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' Responsibilities

Beginning in Section II of the description, the Company has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. The Company is responsible for preparing the description and for the assertion, including the completeness, accuracy, and method of presentation of the description and the assertion, providing the services covered by the description, specifying the control objectives and stating them in the description, identifying the risks that threaten the achievement of the control objectives, selecting the criteria and designing, implementing, and documenting controls to achieve the related control objectives stated in the description.

Ascend Audit & Advisory's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, 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, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period November 1, 2016 to January 31, 2017.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of those controls to achieve the related control objectives stated in the description. 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 achieve the related control objectives stated in the description. Our procedures also included testing the operating effectiveness of those controls that we consider necessary to provide reasonable assurance that the related control objectives stated in the description were achieved. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization and described beginning in Section II. 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, controls at a service organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. 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 achieve the related control objectives is subject to the risk that controls at a service organization may become inadequate or fail.

Opinion

In our opinion, in all material respects, based on the criteria described in the Company's assertion in Section II,

a. the description fairly presents the marketing, print and fulfillment system that was designed and implemented throughout the period November 1, 2016 to January 31, 2017.

b. the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period November 1, 2016 to January 31, 2017 and user entities applied the complementary user entity controls contemplated in the design of the Company's controls throughout the period November 1, 2016 to January 31, 2017.

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 control objectives stated in the description were achieved, operated effectively throughout the period November 1, 2016 to January 31, 2017.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are listed in Section III.

Restricted Use

This report, including 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 information technology, print and fulfillment system during some or all of the period November 1, 2016 to January 31, 2017, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when assessing the risks of material misstatements of user entities' financial statements. 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

February 27, 2017

II. Information Provided by SourceOne Output Technologies

DESCRIPTION OF RELEVANT CONTROLS PROVIDED BY SOURCEONE OUTPUT TECHNOLOGIES

Management Assertions Letter

We have prepared the description of SourceOne Output Technologies' information technology, print and fulfillment system for user entities of the system throughout the period November 1, 2016 to January 31, 2017, and their user auditors who have sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm to the best of our knowledge and belief, that:

a. The description fairly presents the system made available to user entities of the system throughout the period November 1, 2016 to January 31, 2017 for processing their Company's information technology, print and fulfillment system. The criteria we used in making this assertion were that the description:

   i. Presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including:

      1) the types of services provided.
      2) how the system captures and addresses significant events and conditions.
      3) the process used to prepare reports or other information provided to user entities of the system.
      4) specified control objectives and controls designed to achieve those objectives, including complementary user entity controls contemplated in the design of controls.
      5) other aspects of the control environment, risk assessment process, information and communication systems (including the related business processes), control activities, and monitoring controls that are relevant to providing Company's information technology, print and fulfillment system.

   ii. Does not omit or distort information relevant to the scope of Company's information technology, print and fulfillment system, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities, and may not, therefore, include every aspect of the Company's information technology, print and fulfillment system that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. The description includes relevant details of changes to the service organization's system during the period covered by the description when the description covers a period of time.

c. The controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period November 1, 2016 to January 31, 2017 to achieve those control objectives. The criteria we used in making this assertion were that:

   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization,

   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and

   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

By: /S/ Scott Caldarera

Scott Caldarera
Chief Operations Officer

February 27, 2017

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. The company focused on project management from inception to delivery. SourceOne insures the quality and project oversight to help customers develop new projects that often require integrated collateral from multiple vendors and markets. Rapid turnaround times and slow external processes were key drivers for SourceOne to integrate key parts of the delivery cycle in-house.

In 2008, SourceOne Graphics, Inc. transformed itself, rebranding as SourceOne Output Technologies, to clearly define SourceOne as a print-to-mail and electronic file delivery company.

SourceOne Output Technologies continued to maintain all its capabilities and expertise in data processing and intelligent inserting as it grew exponentially, with a 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 fluctuate.

SourceOne Products and Services Overview

USPS Manifest Mailing Approved (Mixed weight presorting)

Weights and thicknesses are calculated based on the number of pages in a set and all accompanying materials for use in sorting. USPS Manifest Mail guidelines are used to ensure best postage rate for mixed weight pieces.

Printing and Mail Methodologies

Multiple workflow methodologies allow for creative variations in types and finishes of final mail pieces. Solutions for any combination and construction:

- Letters, self-mailers, booklet, postcards, magazines, etc.
- Any combination of print, insert, glue, tab, foil stamp

Intelligent Inserts

2-D Barcodes are used throughout the production lifecycle to ensure the accuracy, completeness, and integrity of the job run.

- No missing pages
- No missing envelopes
- No set contamination

2-D Barcode Output Readers assures that pieces are accounted for and are capable of complex read/match/print operations.

Mail Piece Tracking

USPS scan data is automatically parsed and loaded into the tracking system. Data is presented on a mailing by mailing basis through the reporting interface.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT, MONITORING, INFORMATION SYSTEMS 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 way business activities are structured, objectives are established, and risks are assessed. 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 people, 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 Management
- Monitoring

Management Controls, Philosophy, and Operating Style

Management is responsible for directing and controlling operations; establishing, communicating, and monitoring control policies and procedures; as well as 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 help 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 help ensure the highest level of integrity and efficiency in customer support and transaction processing.

Organizational values, ethics, and behavior standards are communicated through formal job descriptions and through regular departmental meetings and staff interactions. 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 to continually monitor the 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 integrity and ethical values in their 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. The Company has developed professional conduct policies that set forth policies of particular 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

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

Commitment to Competence

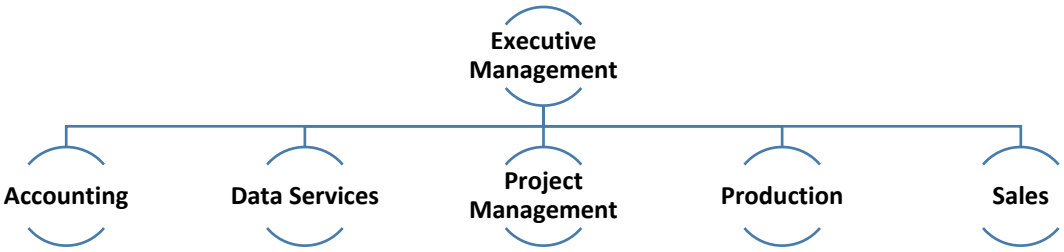
The Company has formal job descriptions that define roles and responsibilities and the experience and background required to perform jobs in a professional and competent fashion. The Company analyzes the knowledge and skills needed to perform job duties and responsibilities and hires for that skill set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

Organization 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 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 the SourceOne corporate structure.



Led by Executive Management, the Company is organized into the following five departments: Accounting; Data Services; Project Management; Production; and Sales.

Assignment of Authority and Responsibility

The control environment is greatly influenced by the extent to which individuals recognize that they will be held accountable. 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 is encouraged as a fundamental part 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.

Accounting Department – is responsible for day-to-day accounting procedures and works closely with each department to ensure accurate processes for documenting all expenses.

Data Services Department – is responsible for taking data supplied by the client or third party companies and processing it to meet USPS mailing standards.

Project Management – is responsible for taking jobs as they have been designed by the Sales Department or the client and documenting all processes needed to get the job completed as designed and on time.

Production Department – is responsible for processing jobs such as printing, folding, binding, inserting, and metering so that the materials are ready to go to the post office for mailing.

Sales Department – is responsible for prospecting for new clients and working with existing clients to produce new and improved methods of reaching their customer base.

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.

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 background investigations relating to past employment history and criminal activity.

The Company invests significant resources in employee development by providing on-the-job training and other learning opportunities. New employees participate in an informal orientation program that acquaints them with SourceOne's organization, 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 area of physical safety and security. Each member of the Company 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 each individual with the understanding and knowledge they need 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.

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 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.

Team leaders are required to identify significant risks related to their areas of responsibility and implement measures to mitigate those risks. The management team, including the President and Chief Operations Officer, 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 all 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. The Company 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 all exceptions to normal processing activities are logged, reported, and resolved.

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 departmental units. Tasks that are not addressed in a timely manner are manually escalated and resolved.

Information Systems

Physical Security

Main Office

SourceOne's headquarters is in a standalone facility located in Little Rock, AR. The grounds surrounding the office and warehouse are secured by commercial fencing. Access to the facility is through one main entrance at the front of the building and two controlled entrances through the side of the building. Visitors are required to sign a visitor log upon entry into the common area. Visitors do not have access to the side entrances as they are secured through push-pin lock access controls.

The Company maintains production computing systems onsite in secured server room. Access to the server room is granted only to the IT Administrator and the Chief Operations Officer.

Server Room Power – The server room is equipped with UPS systems to mitigate the risk of short-term utility power failures and fluctuations. The UPS power provides instantaneous failover in the event of a commercial loss of power.

Server Room Cooling – The server room is equipped with a dedicated cooling units that provide consistent temperature within the server room. Monitoring is in place to notify IT of temperature fluctuations.

Network Perimeter Security

The following are complementary types of network security perimeter devices used by the Company on its network to defend Internet-accessible systems:

- Router
- Firewall
- Network Address Translation (NAT)
- Intrusion Detection System/Intrusion Prevention System (IDS/IPS)
- Virtual Private Network (VPN)

Router

Routers are essential components of the network and control much of the Company's communications. The devices are utilized to divide the network into segments and control traffic flow from one segment to another. Segmenting the network in this manner adds additional levels of security and performance due to the application of traffic flow rules configured on each of the devices. The routers are located in secure, locked rooms to prevent tampering. Logical access to the devices is protected by unique user names and passwords, and can only be utilized by authorized personnel. Additionally, the Company utilizes network monitoring tools to proactively monitor its network for outages.

Firewall

The Company utilizes a firewall at the perimeter of its network to protect against threats from the Internet. The firewall protects the Company's LAN from the WAN environment. The firewall is also used for VPN management for gateway-to-gateway connections as well as gateway-to-user connections.

The firewall device provides user and application policy enforcement, multi-vector attack protection, and secure connectivity services through a wide range of security and networking service in a unified threat management platform including:

- Advanced application-aware firewall services
- Site-to-site and remote access IPSec VPN connectivity
- Intelligent networking services
- Flexible management solutions

Network Address Translation (NAT)

The Company uses the technique of NAT on the main Internet router to provide hidden Internet addresses to internal Company computers. This effectively mitigates the possibility of external sources finding the addresses of internal Company computers.

NAT allows computers on a private network to access the Internet through an intermediary called the Network Address Translator. The Network Address Translator examines all packets destined for the Internet, removes the private IP address from the IP header, substitutes the address of the NAT public interface, and forwards it to the destination. When the resource at the destination IP address responds to the request, the Network Address Translator receives it, checks its internal table to see which client the packet belongs to, and forwards it to the proper client.

Intrusion Detection System/Intrusion Prevention System (IDS/IPS)

The Company utilizes intrusion detection and prevention technology at the perimeter of its network to detect unauthorized access attempts and the presence of malicious code. SourceOne's anti-virus protection software also includes IDS/IPS provisioned at the desktop level. The system is managed and monitored by Company administrators. Alerting has been configured to notify administrators if predefined thresholds are met or exceeded.

An Intrusion Detection System (IDS) detects unwanted manipulations to computer systems, mainly through the Internet. The manipulations may take the form of attacks by hackers.

An IDS is used to detect many types of malicious network traffic and computer usage that cannot be detected by a conventional firewall. This includes network attacks against vulnerable services, data-driven attacks on applications,

host-based attacks such as privilege escalation, unauthorized logins, and access to sensitive files, and malware (viruses, Trojan horses, and worms). An IDS is composed of several components:

- Sensors that generate security events
- A console to monitor events, alerts, and control the sensors
- A central engine that records events logged by the sensors in a database and uses a system of rules to generate alerts from security events received

An Intrusion Prevention System (IPS) is a computer security device that monitors network or system activities for malicious or unwanted behavior and can react in real-time to block or prevent those activities. Network-based IPS, for example, will operate in-line to monitor all network traffic for malicious code or attacks. When an attack is detected, it can drop the offending packets while still allowing all other traffic to pass. Intrusion prevention technology is considered to be an extension of intrusion detection (IDS) technology.

Virtual Private Network (VPN)

A VPN is used to provide secure, encrypted communication between a network and a remote host or other remote networks over the public Internet. VPNs allow the establishment of an encrypted tunnel that protects the flow of network traffic from eavesdroppers.

A VPN is a private encrypted network that uses a public network (usually the Internet) to connect remote sites or users together. Instead of using a dedicated, real world connection such as a leased line, a VPN uses virtual connections routed through the Internet from the private network to the remote site or employee.

Virtual Private Networking is used to allow remote users to access the Company's internal network. Users authenticate with the VPN concentrator and then authenticate with the Windows domain to gain access to network resources. Three levels of access rights and a security device are utilized based on the type of users accessing the network. Strong VPN authentication and encryption protocols are in use.

Computer Operations

Systems Monitoring

The Company regularly monitors the network for capacity, performance, and hardware failure. Overall database health and capacity planning are monitored daily to ensure the system will meet the needs of the Company and its clients. IT monitors 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 system has exceeded a predefined performance or load threshold.
- A system has suffered an error condition.
- A system has detected a hardware element that is expected to fail in the near future.
- A system is no longer in communication with the monitoring infrastructure.
- A system has entered a condition previously specified by Company administrators as operating outside of a threshold.

Patch Deployment

The Company takes a proactive approach to patch management. Company administrators regularly monitor various Web sites and mailing lists where advanced notification of bug and related patches is often disclosed prior to public announcement by the vendor. This allows the Company to plan for upcoming patches.

Company administrators consider each patch carefully and independently to determine if it is necessary to deploy it within the production environment. In many cases, the vulnerability being addressed by the patch has been mitigated through any number of other countermeasures already in place such as firewalls, the intrusion prevention system, or an aspect of their hardening process. In these cases, patches may be deferred until they are included in a future service pack. If Company administrators decide that the patch is necessary and should be deployed, the patch is tested. Once the patch has been thoroughly tested, it is approved for deployment in the production environment.

Logical Access

Access to resource and data are granted to individuals based on their job responsibilities. New user accounts are established only upon receipt of properly authorized requests. The IT Manager is the security administrator and is responsible for ensuring adherence to the security policy that addresses logical access control procedures.

Unique user IDs and passwords are assigned to each individual user. Password rules are established according to the Company security policy, which requires a minimum of alphanumeric characters with password complexity requirements. Passwords are systematically required to be changed periodically. The system administrator sets the user's initial password. The user is required to change the password at first logon.

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

User accounts and access rights are managed on the domain controllers employing the Internet-standard Kerberos network authentication protocol to authenticate both the client and the network, and to protect against the possibility of unauthorized users impersonating a server to enter the network.

Database software maintains their respective client databases. The databases are only accessible through the software application and are protected from unauthorized access. No direct network access is granted to this software or the servers that it runs on to anyone other than those granted by IT management.

Data Backup and Restore

Backup – SourceOne has implemented various backup methods as part of its production operations. The Company has a multi-layered strategy for protecting critical data files to meet business requirements. This strategy includes all data residing on the server backed up to an external hard drive. The drive used for backup is periodically rotated once per week with a drive located in a secure off-site storage location. A log at the offsite location is required for access at any time.

Using an automated process, backup jobs are run using a backup utility whereby the target files are identified in predefined backup jobs. The backup system is monitored continuously by the IT department.

Restore – Restore testing is performed through the course of normal operations and as part of periodic testing. It involves restoring files from backup drives retrieved from the offsite storage vendor.

Disaster Recovery Preparedness

SourceOne takes a mature approach to disaster recovery planning. The Company maintains a formal disaster recovery plan (DRP) that allows for specific recovery times and locations and identifies critical personnel who are integral to the recovery process.

Recovery plan testing takes place in the form of periodic data restores to ensure critical information availability to resume business operations in the event of an extended natural or man-made outage.

Two "footballs" are maintained by the IT Administrator and the Chief Operations Officer. They maintain software licensing, software applications, emergency contact lists, and other components deemed critical to business resumption.

Communication

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; 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 communicate significant events in a timely manner. Employee manuals are provided upon hire that communicate all relevant 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. Periodic departmental meetings between each manager and their staff are held 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 the Company.

Control Objectives and Related Controls

SourceOne's control objectives 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 control objectives and related control activities are included in Section III, they are, nevertheless, an integral part of SourceOne's description of controls.

User Control Considerations

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

This section describes additional controls that should be in operation at user organizations to complement the controls at the Company. User auditors should consider whether or not the following controls have been placed in operation at the 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 job runs are monitored through to completion.
- 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. Processing of transactions for customers by SourceOne covers only a portion of the overall internal control structure of each customer. The Company products and services were not designed to be the only control component in the internal control environment. Additional control procedures are required to be implemented at the customer level. It is not feasible for all of the control objectives relating to the processing of transactions to be completely 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

CONTROL OBJECTIVES, RELATED CONTROLS, AND TESTS OF OPERATING EFFECTIVENESS

Control Objective 1 – Organization and Administration

CO1 – Controls provide reasonable assurance that management provides oversight, segregation of duties, and guides consistent implementation of security practices.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.1	The Company has a corporate information security program that guides personnel on procedures and policies to ensure information security within the organization.	Inspected the corporate security program documentation to determine the Company had a corporate information security program that guided personnel on procedures and policies to ensure information security within the organization.	No exceptions noted.
C1.2	An organizational chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and is updated on a periodic basis.	Inspected the current organizational chart to determine it was in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel and it was updated on a periodic basis.	No exceptions noted.
C1.3	An acceptable use policy is in place that guides staff on the appropriate use of Company computers, information systems, and adherence to security policies.	Inspected the acceptable use policy to determine it was in place to guide staff on the appropriate use of Company computers, information systems, and adherence to security policies.	No exceptions noted.
C1.4	The Company has documented job descriptions that describe the roles and responsibilities of the position.	Inspected a selection of job descriptions to determine they were in place and described the roles and responsibilities of the position.	No exceptions noted.

Control Objective 1 – Organization and Administration (Continued)

CO1 – Controls provide reasonable assurance that management provides oversight, segregation of duties, and guides consistent implementation of security practices.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C1.5	Management ensures employees are subjected to a criminal background check during the hiring process.	Informed by SourceOne management that there were no new hires to the organization during the period under review.	No testing performed.
C1.6	New employees must sign a confidentiality and nondisclosure agreement as acknowledgement not to disclose proprietary or confidential information, including client information, to unauthorized parties.	Informed by SourceOne management that there were no new hires to the organization during the period under review.	No testing performed.
C1.7	The Company has an employee handbook that describes management's philosophy and operating style and provides HR policy guidance to employees.	Inspected the employee handbook to determine that the Company had an employee handbook that described management's philosophy and operating style and provided HR policy guidance to employees.	No exceptions noted.

Control Objective 2 – Information Security: Logical Access

CO2 – Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.1	SourceOne users are authorized for network access and the authorization is documented and approved prior to provisioning. Users are assigned the appropriate rights for their role.	Informed by SourceOne management that there were no new hires to the organization during the period under review.	No testing performed.
C2.2	A new hire checklist is completed to ensure a standardized on-boarding procedure for each new hire.	Informed by SourceOne management that there were no new hires to the organization during the period under review.	No testing performed.
C2.3	Password settings are consistent with the security policy. Passwords must conform to the following minimum requirements as enforced by the network operating system: • Minimum length • Complexity requirements • Reuse history • Maximum age • Invalid logon attempt lockout	Inspected the password policy to determine it was consistent with and conformed to the following minimum requirements as enforced by the network operating system: • Minimum length • Complexity requirements • Reuse history • Maximum age • Invalid logon attempt lockout	No exceptions noted.
C2.4	User accounts are disabled at time of termination. Depending on the user profile, the account is either disabled or the password is changed and email is forwarded to the manager.	Informed by SourceOne management that there were no terminations from the organization during the period under review.	No testing performed.

Control Objective 2 – Information Security: Logical Access (Continued)

CO2 – Controls provide reasonable assurance that logical access to programs, data, and computer resources is restricted to authorized and appropriate users, and such users are restricted to performing authorized and appropriate actions.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C2.5	Management utilizes and retains termination checklists as a confirmation of the revocation of system and facility access privileges as a component of the employee termination process.	Informed by SourceOne management that there were no new terminations of the organization during the period under review.	No testing performed.
C2.6	SourceOne security groups are configured and enforced by the network operating system and servers to ensure access is restricted to sensitive data stored on the network.	Inspected a screenshot of the Active Directory security groups to determine SourceOne security groups were configured and enforced by the network operating system and servers to ensure access was restricted to sensitive data stored on the network.	No exceptions noted.
C2.7	Network security event logging is configured to log specific events on the network domain.	Inspected the network domain audit settings and event logs on domain controllers to determine network security event logging was configured to log specific events on the network domain.	No exceptions noted.

Control Objective 3 – Information Security: Physical Access

CO3 – Controls provide reasonable assurance that physical access to computer and other resources is restricted to authorized and appropriate personnel.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C3.1	Physical access to SourceOne's facilities is restricted via secured controls.	Inspected the physical access system's activity logs to determine physical access to SourceOne's facilities was restricted via secured controls.	No exceptions noted.
C3.2	Physical access to media is controlled and unauthorized access is detected.	Inspected digital evidence and conducted corroborative inquiry of IT management to determine physical access to media was controlled and unauthorized access was detected.	No exceptions noted.
C3.3	SourceOne's data center access is restricted to only authorized personnel.	Inspected the data center access control list to determine SourceOne's data center access was restricted to only authorized personnel.	No exceptions noted.
C3.4	Visitors are required to sign in on a visitor log at the main entrance upon arrival and are accompanied by a Company employee during their visit.	Observed via walkthrough procedures, the visitor log to determine visitors were required to sign in on a visitor log at the main entrance upon arrival and were accompanied by a Company employee during their visit.	No exceptions noted.

Control Objective 4 – Information Security: Environmental Controls

CO4 – Controls provide reasonable assurance that systems are in place to alert and affect certain environmental risks.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C4.1	The facility has a fire suppression system in place that is maintained and inspected periodically.	Inspected the handheld fire extinguisher inspection tags to determine the facility had a fire suppression system in place that was maintained and inspected periodically.	No exceptions noted.
C4.2	The data center is equipped with dedicated HVAC systems used to control temperature and humidity.	Observed via walkthrough procedures and digitally recorded, the configuration of HVAC systems to determine the data center was equipped with dedicated HVAC systems used to control temperature and humidity.	No exceptions noted.
C4.3	An uninterruptible power supply (UPS) system is in place to provide alternate power in the event of a momentary interruption in commercial power.	Observed via walkthrough procedures and digitally recorded, the UPS system to determine a UPS system was in place to provide alternate power in the event of a momentary interruption in commercial power.	No exceptions noted.
C4.4	A generator is in place to provide power in the event of an extended disruption to commercial power.	Observed via walkthrough procedures and digitally recorded, the backup generator configuration to determine a generator was in place to provide power in the event of an extended disruption to commercial power.	No exceptions noted.
C4.5	The generator is inspected and serviced at least annually by third-party vendors to ensure effective operation.	Inspected the generator maintenance and test logs to determine the generator was inspected and serviced by third-party vendors to ensure effective operation, during the period under review.	No exceptions noted.

Control Objective 5 – Computer Operations

CO5 – Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C5.1	A firewall is in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	Inspected the firewall configuration to determine a firewall was in place to control network traffic and prevent unauthorized traffic from passing between the internal network and external networks.	No exceptions noted.
C5.2	Management restricts the ability to administer the firewall systems and network communications equipment to certain personnel.	Inspected the firewall access control list to determine administrative access to communications devices was restricted to certain authorized personnel.	No exceptions noted.
C5.3	The firewall is configured to automatically terminate authenticated sessions if predefined inactivity thresholds are exceeded.	Inspected the firewall configuration to determine the firewall was configured to automatically terminate authenticated sessions if predefined inactivity thresholds were exceeded.	No exceptions noted.
C5.4	The firewall is configured to generate activity logs when certain firewall events occur.	Inspected logs from the firewall to determine the firewall was configured to generate activity logs when certain firewall events occurred.	No exceptions noted.
C.5.5	SourceOne's patch management includes continually updating critical servers once system administrators approve and test recommended patches.	Inspected a screenshot of the system and security patch history to determine critical servers were continually updated. *Exception noted*: There was no evidence of one critical server being updated on a continually basis. *Management response*: Server has been updated and configured for continual updating as of this finding.	Exception noted.

Control Objective 5 – Computer Operations (Continued)

CO5 – Controls provide reasonable assurance that application and system processing are authorized and executed in a complete, accurate, and timely manner, and deviations, problems, and errors are identified, tracked, recorded, and resolved in a complete, accurate, and timely manner.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C5.6	Anti-virus software is configured to automatically update servers and personal computers on a daily basis.	Inspected a screenshot of the anti-virus software configurations to determine anti-virus software was in place and configured to automatically update servers and personal computers on a daily basis.	No exceptions noted.
C5.7	Network Address Translation (NAT) services are enabled on the network firewalls. Internal production servers do not have routable IP addresses.	Inspected the IP address scheme of the production servers to determine NAT services were enabled on the network firewall, and internal production servers did not have routable IP addresses.	No exceptions noted.
C5.8	An Intrusion Prevention System (IPS) is utilized to monitor the network 24x7x365 for malicious activity and unauthorized access attempts. The IPS is configured to alert administrators when predefined thresholds are exceeded regarding access attempts and malicious code.	Inspected screenshots of the IPS configuration to determine an IPS was in place, monitored the network continuously, and provided alerts to administrators when predefined thresholds were exceeded regarding access attempts and malicious code.	No exceptions noted.

Control Objective 6 – Data Transmission

CO6 – Controls provide reasonable assurance that data transmission between service organization and its user entities and other outside entities are from authorized sources and are complete, accurate, secure, and timely.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C6.1	Secure File Transfer Protocol (SFTP) is utilized for securing sensitive data transmission.	Inspected screenshots of the SFTP interface and configuration to determine SFTP was utilized for securing sensitive data transmission.	No exceptions noted.
C6.2	Systematic notifications are distributed by the SFTP server for monitoring the success or failure of transactions.	Inspected screenshots of completed notification logs to determine systematic notifications were distributed by the SFTP server for monitoring the success or failure of transactions.	No exceptions noted.

Control Objective 7 – Backup and Data Recovery

CO7 – Controls provide reasonable assurance that data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C7.1	Automated backup systems are utilized to perform scheduled system backups of target data.	Inspected a daily backup report to determine an automated backup system was utilized to perform scheduled system backups of target data.	No exceptions noted.
C7.2	Backup jobs are monitored and notification alerts are sent in the event of backup failure.	Inspected backup alert notifications to determine backup jobs were monitored and notification alerts were sent in the event of backup failure.	No exceptions noted.
C7.3	Backup media containing target data is encrypted to prevent unauthorized access.	Inspected the encryption settings in the backup software to determine that backup media containing target data was encrypted to prevent unauthorized access.	No exceptions noted.
C7.4	Backup media access is restricted to only authorized personnel.	Inspected the access control list of the backup software to determine access was restricted to only personnel with administrative access.	No exceptions noted.
C7.5	The backup application performs automated daily incremental and weekly full backups.	Inspected a sample backup report to determine the backup application performed automated daily incremental and weekly full backups.	No exceptions noted.
C7.6	Tape transfer logs are maintained to document the transfer of backup media to the offsite facility.	Inspected tape transfer logs to determine personnel maintained tape transfer logs to document the transfer of backup media to the offsite facility.	No exceptions noted.

Control Objective 7 – Backup and Data Recovery (Continued)

CO7 – Controls provide reasonable assurance that data is backed up regularly and is available for restoration in the event of processing errors or unexpected processing interruptions.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C7.7	Restore testing is performed through the course of normal operations as part of periodic testing.	Inspected a screenshot of the backup restore application console to determine restore testing was performed through the course of normal operations as part of periodic testing.	No exceptions noted.

Control Objective 8 – Disaster Recovery Preparedness

CO8 – Controls provide reasonable assurance that orders are processed, fulfilled, and shipped in a timely and accurate manner.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C8.1	Management maintains a disaster recovery plan (DRP) to facilitate disaster recovery operations and includes procedures for declaring a disaster, plan administration, offsite inventory recovery, recovery time frames, recovery actions, and network recovery.	Inspected the DRP to determine a DRP was in place to facilitate disaster recovery operations and included procedures for declaring a disaster, plan administration, offsite inventory recovery, recovery time frames, recovery actions, and network recovery.	No exceptions noted.
C8.2	The DRP is tested at least annually.	Inspected the DRP test results to determine the DRP was tested at least once during the period under review.	No exceptions noted.
C8.3	SourceOne maintains a hot site with matching equipment used by SourceOne so printing operations could begin as early as the next business day in this temporary location.	Inspected the hot site third-party documentation to determine SourceOne printing operations could begin as early as the next business day in this temporary location.	No exceptions noted.

Control Objective 9 – Order Processing, Fulfillment and Shipping

CO9 – Controls provide reasonable assurance that orders are processed, fulfilled, and shipped in a timely and accurate manner.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C9.1	A logistics tracking system is in place for the management of order and fulfillment processing.	Observed via walkthrough procedures, the logistic tracing system to determine it was in place and utilized for the management of order and fulfillment processing.	No exceptions noted.
C9.2	Clients are required to acknowledge and approve proofs prior to production.	Inspected a sample of approved and completed proofs to determine clients were required to acknowledge and approve proofs prior to production.	No exceptions noted.
C9.3	Acceptance testing is performed for any required changes to orders.	Inspected a sample of completed job control tickets to determine acceptance testing was performed for required changes to orders.	No exceptions noted.
C9.4	The job order process is tracked through to completion.	Inspected a sample of completed job tickets containing work instructions and approvals to determine the job order process was tracked through completion.	No exceptions noted.
C9.5	USPS mail counts are verified by the onsite USPS postal clerk.	Via walkthrough, inspected the mail count verification process to determine the USPS postal clerk reconciled and acknowledged the original mail count log supplied by loading dock personnel.	No exceptions noted.
C9.6	Job order non-conformity reports and procedures are in place to identify and manage non-conformities of production runs.	Inspected a sample of non-conformity reports and the non-conformity procedures to determine job order non-conformity reports and procedures were in place to identify and manage non-conformities of production runs.	No exceptions noted.

Control Objective 9 – Order Processing, Fulfillment and Shipping (Continued)

CO9 – Controls provide reasonable assurance that orders are processed, fulfilled, and shipped in a timely and accurate manner.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C9.7	Drivers are required to count and reconcile physical counts to the systematically generated packing slip.	Inspected a sample of pickup and delivery (P&D) reconciliation reports to determine drivers were required to count and reconcile physical counts to the systematically generated packing slip.	No exceptions noted.

Control Objective 10 – Inventory Audit

CO10 – Controls provide reasonable assurance that inventory audits are completed to prevent inventory errors.

	Controls Specified by SourceOne	Testing Performed by Ascend Audit & Advisory	Results of Tests
C10.1	An internal audit function exists to perform inventory audits on a scheduled basis.	Inspected a sample of inventory audit reports to determine an internal audit function existed to perform inventory audits on a scheduled basis.	No exceptions noted.
C10.2	A daily analysis is performed for inventory errors.	Observed inventory error reports and conducted corroborative inquiry of management to determine a daily analysis was performed for inventory errors.	No exceptions noted.