Hiestand, Brand, Loughran, P.A.

SOC 2 Type 2 Report on Controls Relevant to Security, Availability, and Confidentiality for Printing, Mailing, and Fulfillment Services

Shapco Printing, Inc.

May 16, 2017 to April 30, 2018

An Affiliate Company of
360ADVANCED

SHAPCO PRINTING, INC.

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT ON A DESCRIPTION OF A SERVICE ORGANIZATION'S SYSTEM AND THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY

To Shapco Printing, Inc.:

Scope

We have examined the description of Shapco Printing, Inc.'s ("Shapco") Printing, Mailing, and Fulfillment Services system based on the criteria set forth in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria) and the suitability of the design and operating effectiveness of controls described therein to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A, *Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services criteria), throughout the period May 16, 2017 to April 30, 2018.

The description indicates that certain applicable trust services criteria specified in the description can be met only if complementary user entity controls assumed in the design of Shapco's controls are suitably designed and operating effectively, along with the related controls of the service organization. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls. The controls included in the description are those that management of Shapco believes are likely to be relevant to meeting the applicable trust services criteria, and the description does not include those aspects of the Printing, Mailing, and Fulfillment Services system that are not likely to be relevant to meeting the applicable trust services criteria.

Service Organization's Responsibilities

Within Section 2 of this report, Shapco has provided an assertion about the fairness of the presentation of the description based on the description criteria and suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria. Shapco is responsible for (1) preparing the description and assertion; (2) including the completeness, accuracy, and method of presentation of the description and assertion; (3) providing the services covered by the description; (4) identifying the risks that would prevent the applicable trust services criteria from being met; (5) designing, implementing, and documenting the controls to meet the applicable trust services criteria; and (6) specifying the controls that meet the applicable trust services criteria and stating them in the description.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the fairness of the presentation of the description based on the description criteria and the suitability of the design and operating effectiveness of the controls described therein to meet the applicable trust services criteria, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants, and, accordingly, included procedures that we considered necessary in the circumstances. 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 May 16, 2017 to April 30, 2018.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of the controls to meet the applicable trust services criteria involves:

- evaluating and performing procedures to obtain evidence about whether the description is fairly presented based on the description criteria, and the controls were suitably designed and operating effectively to meet the applicable trust services criteria throughout the period May 16, 2017 to April 30, 2018

- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively
- testing the operating effectiveness of those controls to provide reasonable assurance that the applicable trust services criteria were met
- evaluating the overall presentation of the description, the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization in its assertion

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

In our opinion, in all material respects, based on the description criteria identified in Shapco's assertion and the applicable trust services criteria:

a. the description fairly presents the system that was designed and implemented throughout the period May 16, 2017 to April 30, 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 May 16, 2017 to April 30, 2018, and user entities applied the complementary user entity controls assumed in the design of Shapco's controls throughout the period May 16, 2017 to April 30, 2018
c. the controls tested operated effectively to provide reasonable assurance that the applicable trust services criteria were met throughout the period May 16, 2017 to April 30, 2018 if the user entities applied the complementary user entity controls assumed in the design of Shapco's controls, and those controls operated effectively throughout the period May 16, 2017 to April 30, 2018

Description of Tests of Controls

The specific controls we tested, the tests we performed, and the results of our tests are presented in Section 4 of this report.

Restricted Use

This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Shapco and user entities of Shapco's Printing, Mailing, and Fulfillment Services system during some or all of the period May 16, 2017 to April 30, 2018; and prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities and other parties
- Internal control and its limitations
- The nature of user entity controls and responsibilities, and their role in the user entities internal control as they relate to, and how they interact with, related controls at the service organization 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.

June 11, 2018
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

June 11, 2018

We have prepared the description of Shapco Printing, Inc.'s ("Shapco") Printing, Mailing, and Fulfillment Services system based on the criteria for a description of a service organization's system identified in paragraph 1.26 of the AICPA Guide, *Reporting on Controls at a Service Organization: Relevant to Security, Availability, Processing Integrity, Confidentiality, or Privacy (SOC 2®)* (description criteria). The description is intended to provide users with information about the Printing, Mailing, and Fulfillment Services, particularly system controls intended to meet the criteria for the Security, Availability, and Confidentiality principles set forth in TSP section 100A*, Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (applicable trust services principles), throughout the period May 16, 2017 to April 30, 2018. We confirm, to the best of our knowledge and belief, that

1) The description fairly presents the Printing, Mailing, and Fulfillment Services system throughout the period May 16, 2017 to April 30, 2018. Our assertion is based on the following description criteria:
    a) 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 structures, IT and other hardware
            - *Software* - the application programs and IT system software that supports application programs
            - *People* - the personnel involved in the governance, operation, and use of a system
            - *Procedures* - the automated and manual procedures
            - *Data* – transaction streams, files, databases, tables, and output used or processed by the system
        3. the boundaries or aspects of the system covered by the description
        4. for information provided to, or received from, sub-service organizations, and other parties:
            a. how such information is provided or received and the role of the sub-service organization and other parties
            b. the procedures the service organization performs to determine that such information and its processing, maintenance, and storage are subject to appropriate controls
        5. the applicable trust services criteria and related controls designed to meet those criteria, including, as applicable, the following:
            a. complementary user entity controls contemplated in the design of the service organization's system
            b. when the inclusive method is used to present a sub-service organization, controls at the sub-service organization
        6. if the service organization presents the sub-service organization using the carve-out method:
            a. the nature of the services provided by the sub-service organization

b. each of the applicable trust services criteria that are intended to be met by controls at the sub-service organization, alone or in combination with controls at the service organization, and the types of controls expected to be implemented at carved-out sub-service organizations to meet those criteria

7. any applicable trust services criteria that are not addressed by a control at the service organization or a sub-service organization and the reasons
8. relevant details of changes to the service organization's system during the period covered by the description

b) The description does not omit or distort information relevant to the service organization'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.

2) The controls in the description were suitably designed throughout the period May 16, 2017 to April 30, 2018, to meet the applicable trust services criteria.

3) The controls stated in the description operated effectively throughout the period May 16, 2017 to April 30, 2018, to meet the applicable trust services criteria.

/s/ Shapco Printing, Inc.

Joel Shapiro – CEO / President

Paresh Patel – VP of Technologies

SECTION 3:

SHAPCO'S DESCRIPTION OF CONTROLS

SCOPE OF REPORT AND DISCLOSURES

Overview

This description of the system of controls provided by Shapco Printing, Inc.'s ("Shapco") management, as related to Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, '*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Examination Engagements*,' considers the direct and indirect impact of risks and controls that Shapco's management has determined are likely to be relevant to its user entities' internal controls intended to mitigate risks related to security, availability, processing integrity, confidentiality, or privacy.

Principles and Related Criteria

The five attributes of a system are known as *principles*, and they are defined as follows:

- **Security**: The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements. The *security principle* refers to the protection of the system resources through logical and physical access control measures in order to enable the entity to meet its commitments and system requirements related to security, availability, processing integrity, confidentiality, and privacy. Controls over the security of a system prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of data or system resources, misuse of software, and improper access to, or use of, alteration, destruction, or disclosure of information.
- **Availability**: The system is available for operation and use to meet the entity's commitments and system requirements. The *availability principle* refers to the accessibility of the system, products, or services as committed by contract, service-level agreement, or other agreements. This principle does not, in itself, set a minimum acceptable performance level for system availability. The *availability principle* does not address system functionality (the specific functions a system performs) and system usability (the ability of users to apply system functions to the performance of specific tasks or problems), but does address whether the system includes controls to support system accessibility for operation, monitoring, and maintenance.
- **Processing Integrity**: System processing is complete, valid, accurate, timely, and authorized to meet the entity's commitments and system requirements. The *processing integrity principle* refers to the completeness, validity, accuracy, timeliness, and authorization of system processing. Processing integrity addresses whether the system achieves its aim or the purpose for which it exists, and whether it performs its intended function in an unimpaired manner, free from unauthorized or inadvertent manipulation. Processing integrity does not automatically imply that the information received and stored by the system is complete, valid, accurate, current, and authorized. The risk that data contains errors introduced prior to its input in the system often cannot be addressed by system controls and detecting such errors is not usually the responsibility of the entity. Similarly, users outside the boundary of the system may be responsible for initiating processing. In these instances, the data may become invalid, inaccurate, or otherwise inappropriate even though the system is processing with integrity.
- **Confidentiality**: Information designated as confidential is protected to meet the entity's commitments and system requirements. The *confidentiality principle* addresses the system's ability to protect information designated as confidential, including, its final disposition and removal from the system in accordance with management's commitments and system requirements. Information is confidential if the custodian of the information is required to limit its access, use, and retention, and restrict its disclosure to defined parties. Such requirements may be contained in laws or regulations, or commitments in user contracts. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel. Confidentiality is distinguished from privacy in that privacy only applies to personal information, while the confidentiality principle applies to various types of sensitive information. In addition, the privacy principle addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information.

Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

- **Privacy**: Personal information is collected, used, retained, disclosed, and disposed to meet the entity's commitments and system requirements.

Many of the criteria used to evaluate a system are shared amongst all of the principles; for example, the criteria related to risk management apply to the security, availability, processing integrity, confidentiality, and privacy principles. As a result, the trust services criteria of (1) criteria common to all five principles (common criteria) and (2) additional principle specific criteria for the availability, processing integrity, confidentiality, and privacy principles. For the security principle, the common criteria constitute the complete set of criteria. For the principles of availability, processing integrity, confidentiality, and privacy, a complete set of criteria consists of the common criteria and the criteria applicable to the principles addressed by the engagement. The criteria for a principle addressed by the engagement are considered to be complete only if all of the criteria associated with that principle are addressed by the engagement.

The common criteria are organized into seven categories:

a. *Organization and management.* The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principles addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.

b. *Communications*. The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and system requirements to authorized users and other parties of the system to meet the criteria for the principles addressed by the engagement.

c. *Risk management and design and implementation of controls.* The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process to meet the criteria for the principles addressed by the engagement.

d. *Monitoring of controls.* The criteria relevant to how the entity monitors the system, including the suitability of the design and operating effectiveness of the controls, and takes action to address deficiencies identified to meet the criteria for the principles addressed by the engagement.

e. *Logical and physical access controls.* The criteria relevant to how the entity restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principles addressed in the engagement.

f. *System operations.* The criteria relevant to how the entity manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the criteria for the principles addressed in the engagement.

g. *Change management*. The criteria relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principles addressed in the engagement.

Although the confidentiality principle applies to various types of sensitive information, the privacy principle applies only to personal information. If the entity is directly responsible for providing services to data subjects covering all of the categories noted as follows, then the privacy principle may be appropriate. If the entity is not directly responsible for significant aspects of the following categories but retains responsibility for protecting personal information, the confidentiality principle may be more applicable.

The privacy criteria are organized into eight categories:

a. *Notice and communication of commitments and system requirements.* The entity provides notice to data subjects about its privacy practices, its privacy commitments, and system requirements.

b. *Choice and consent.* The entity communicates choice available regarding the collection, use, retention, disclosure, and disposal of personal information to data subjects.

c. *Collection.* The entity collects personal information to meet its privacy commitments and system requirements.

d. *Use, retention, and disposal.* The entity limits use, retention, and disposal of personal information to meet its privacy commitments and system requirements.

e. *Access.* The entity provides data subjects with access to their personal information for review and correction (including updates) to meet its privacy commitments and system requirements.

f. *Disclosure and notifications.* The entity discloses personal information, with the consent of the data subjects, to meet its privacy commitments and system requirements. Notification of breaches and incidents is provided to affected data subjects, regulators, and others to meet its privacy commitments and system requirements.

g. *Quality.* The entity collects and maintains accurate, up-to-date, complete, and relevant personal information to meet its privacy commitments and system requirements.

h. *Monitoring and enforcement.* The entity monitors compliance to meet its privacy commitments and system requirements including procedures to address privacy-related inquiries, complaints, and disputes.

The scope management has determined appropriate for the Printing, Mailing, and Fulfillment Services system includes the controls to meet the criteria for the Security, Availability, and Confidentiality principles. Shapco is responsible for identification of risks associated with the system of controls (defined as Principles), and for the design and operation of controls intended to provide reasonable assurance that the applicable trust services criteria would be met.

As part of its overall SOC 2 program, Shapco management sets and determines the scope and timing of each report. This description of the system has been prepared by Shapco management to provide information on controls applicable to meet the criteria for the Security, Availability, and Confidentiality principles for the Minneapolis, Minnesota facility.

Sub-Service Organizations

Shapco Printing, Inc. does not rely on any sub-service organizations as part of the Printing, Mailing, and Fulfillment Services system included in the scope of this report.

Significant Changes during the Examination Period

Management is not aware of any significant changes that occurred during the examination period.

Subsequent Events

Management is not aware of any relevant events that occurred subsequent to the period covered by management's description included in Section 3 of this report through the date of the service auditor's report that would have a significant effect on management's assertion.

Using the Work of the Internal Audit Function

The service auditor did not utilize any work of an Internal Audit function in preparing this report.

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

Shapco was founded in 1976 by the Shapiro family with the vision that a printing company could succeed by crafting rather than merely manufacturing a printed product. Since that time the company has grown to approximately 120 employees serving multiple industries and clients across North America. Shapco provides: conventional printing, digital printing, large format printing, books, packaging, annual reports, ultra-violet (UV), kitting, finishing and direct mailing. Shapco operates from its print facility located in Minneapolis, Minnesota which includes 80,000 square feet for dedicated printing activities and a 360 square foot data center.

Overview of Printing, Mailing, and Fulfillment Services System

Shapco's Printing, Mailing, and Fulfillment Services system includes for the following forms of service:

- **Prepress** – The ability for clients to upload files to Shapco's secure site or scan them using a high-resolution drum or flatbed scanner. Shapco prepares the client's files and sends the client a soft proof and a realistic proof from their system using real ink dyes.
- **Conventional** – Conventional printing services, as well as two eight-color, and one six-color UV presses allowing for the addition of coatings.
- **UV** – The two eight-color, and one six-color UV presses print UV inks on paper, plastic or other substrates up to 40 points thick.
- **Digital Printing**:
    - Variable data including tailored printing to include custom colors, photos or text to individuals in the mailing lists.
    - Point-of-purchase displays, booth graphics, decals, banners, outdoor signage on paper, vinyl or other substrates, accommodating 96 inch to 120 inch wide capability with multiple colors.
    - Direct mail capability to individuals or geographic areas on client mailing lists.
- **Finishing** – Cutting, folding, gluing, binding, assembling, and kiting print jobs.
- **Mailing and Fulfillment** – Managing clients' databases, sealing and metering pieces, and drop-shipping them.

OVERVIEW OF RELEVANT INFRASTRUCTURE

The Printing, Mailing, and Fulfillment Services system is comprised of the following components:

- Infrastructure – the physical structures, IT, and other hardware
- Software – the application programs and IT system software that supports application programs
- People – the personnel involved in the governance, operation, and use of a system
- Procedures – the automated and manual procedures
- Data – transaction streams, files, databases, tables, and output used or processed by the system

Infrastructure

Shapco's local information systems are run on Microsoft Windows file servers. Employees access the network and applications either through their:

- Company supplied Microsoft Windows desktop computers
- Apple desktop company supplied computers
- Through an encrypted secure virtual private network (VPN) using Advanced Encryption Standard 256-bit encryption

Information systems consist of a combination of internally hosted and managed applications and cloud hosted and managed applications. In addition, support and maintenance of desktop and server systems is provided by internal IT staff that maintains administrative control over the applications and underlying technical infrastructure.

The following describes the in-scope components supporting the Printing, Mailing, and Fulfillment Services system:

System / Application	Description	Infrastructure
Monarch	Enterprise Resource Planning (ERP)	Windows 2012 R2, SQL 2012
BCC - Bell & Howell Mail Manager	Mail management	Windows 7 Desktop
Adobe Creative Suite (CS)	Graphic design	Cloud Solution, Mac
SolarWinds	Enterprise monitoring	Windows 2012 R2, SQL 2012
Storefront websites	Client specific websites for ordering client printing and fulfillment.	Windows 2012 R2, SQL 2012

Software

- **Monarch** – Monarch is a purchased application which is hosted and managed internally by Shapco. Monarch is Shapco's ERP application including: client credit authorizations, client orders, inventory management, shipping, receiving, job scheduling, and financial management.

  Access to Monarch is based on business need and requires a valid user ID and password.

- **BCC - Bell & Howell Mail Manager** – BCC is a purchased application which is hosted and managed internally by Shapco. BCC is a mail management application that delivers a suite of mail preparation functionality, including automation of workflow. Shapco utilizes BCC for: address standardization, address corrections (National Change of Address - NCOA), postal automation, statement processing, etc.

  Access to BCC is based on business need and requires a valid user ID and password.

- **Adobe Creative Suite (CS)** – Adobe CS is a purchased application which is hosted and managed by Adobe as a cloud solution (Adobe Creative Cloud). Adobe CS is a series of software applications utilized for graphic design. The collection of application consists of various groupings of Adobe's applications (e.g., Photoshop, Acrobat, InDesign, Premiere Pro, After Effects). Shapco utilizes Adobe CS in its Prepress operations.

  Access to Adobe CS is based on business need and requires a valid user ID, password, and predefined license authorization.

- **SolarWinds** – SolarWinds is a purchased application which is hosted and managed internally by Shapco. SolarWinds is a suite of network, server, and system monitoring tools for the management of the enterprise networked system. Shapco utilizes SolarWinds to monitor and manage its internally supported systems.

  Access to SolarWinds is confined to internal and select external system support personnel and contractors through valid user ID and password.

- **Storefront Websites** – Shapco designs and implements client specific websites for ordering printing directly from the clients. Through these websites, clients can order print services directly. Client storefronts are pre-authorized and pre-designed. Each client user must be pre-authorized by the client's management prior to being issued of a unique user ID and password to the storefront website. Clients only have access to view and order products that are unique to their company and are expected to manager their own user's access.

People

Shapco has a staff of approximately 120 employees and is organized in the following functional areas:

Business Function	Functional Responsibility
Accounting	Responsible for the financial aspects of Shapco.
Human Resources	Responsible for managing personnel related activities, including recruiting and retention of talent, training, etc.
Information Technology	Responsible for application systems and technical infrastructure and managing the relationship with the third-party IT support providers.
Sales & Marketing	Responsible for development and promotion of services available from the organization.
Prepress	Responsible for pre-flight files, imposing and preparing files for production, ensuring color integrity, and outputting proofs, PDF's, or plates.

Business Function	Functional Responsibility
Digital Printing	Responsible for the printing of digital-based image directly to the media. This group is responsible the importing of data from clients and confirming quality of printed documents.
Conventional Printing	Responsible for the printing on high speed commercial printing equipment. This group is responsible for confirming quality of printed documents.
Bindery Services	Responsible for the finishing activities (e.g., binding, cutting, folding, and gluing).
Fulfillment	Responsible for storing finished goods on behalf of clients and utilizes finished goods to perform fulfillment activities. Example activities include: kitting and assembly.
Mailing Services	Responsible for converting data files for imaging data on paper documents, for inserting printed and paper documents into envelopes, applying postage, using modern postal technology in preparation for distribution processes.

The organizational structure of Shapco provides the framework for establishing organization goals and ensuring resources are available to perform printing, mailing, and fulfillment services. Performance and quality of these services is the responsibility of the Senior Management team.

Management of Shapco is responsible for directing and controlling operations related to its services and for establishing, communicating, and monitoring control policies and procedures. The organization emphasizes integrity and ethical values of Shapco personnel and the importance of maintaining sound internal controls.

The hierarchy and reporting structure of Shapco has been established to support its strategic objectives and to promote its operational independence from other functions. The organization structure of Shapco provides the overall framework for planning, directing, and controlling operations for its services and uses an approach whereby personnel are segregated based on job responsibilities.

Updates to the organization chart are made by the organization as necessary based on position changes approved by the CEO / President.

Procedures

Changes to procedures are performed at least annually and are authorized by senior management. These procedures cover the following key security lifecycle areas:

- Data classification (data at rest, in motion and output)
- Categorization of information
- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles

- Maintenance and support of the security system and necessary back-ups and offline storage
- Incident response
- Maintenance of restricted access to system configurations, super user functionality, master passwords, powerful utilities, and security devices (for example, firewalls.)

Data

Shapco manages the print, mail, and fulfillment operations within its IT infrastructure environment. Access to data is limited to authorized personnel in accordance with Shapco security policies. Shapco is responsible for the overall availability of data, including system backups, monitoring of data processing and file transmissions as well as identifying and resolving problems.

Management has classified data into the following:

- Transaction data
- Print jobs
- Printed materials
- Electronic interface files
- Output reports
- Input reports
- System files
- Error logs

RELEVANT ASPECTS OF CONTROL ENVIRONMENT, RISK ASSESSMENT, INFORMATION AND COMMUNICATIONS SYSTEMS, MONITORING, POLICIES AND PRACTICES

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 controls, providing discipline and structure. Aspects of Shapco's control environment that affect the services provided and / or the system of controls are identified in this section.

Integrity and Ethical Values

The effectiveness of controls is greatly influenced by the level of integrity and ethical values of the people who create, administer, and monitor them. Integrity and ethical values are important elements of Shapco control environment, affecting the design, administration, and monitoring of other components. The communication and implementation of ethical behavior throughout the organization is designed to reduce the likelihood of personnel to engage in dishonest, illegal, or unethical acts.

Shapco enforces high ethical standards in all levels of communication to and through its employees. Shapco continuously audits its employees' communication with client and outside resources to ensure compliance with these standards and addresses any issues as soon as they arise. Shapco emphasizes high standards during its interpersonal communications via meetings, email and phone calls. Any questionable acts are dealt with immediately and positive acts are recognized and acknowledged in public forums in an effort to reinforce positive / constructive behaviors. Employees who violate these standards are disciplined according to company policies.

Board of Directors / Executive Management

Shapco's control consciousness is influenced significantly by its Executive Management team. Attributes include the experience and stature of its members, the extent of its involvement and scrutiny of activities, the appropriateness of its actions, the degree to which difficult questions are raised and pursued with management and staff, and its interaction with external auditors. The Executive Management team includes the company's CEO / President and key executive members.

Commitment to Competence

Management has established a framework for the basic skills necessary to perform each of the jobs at Shapco. This framework is then augmented with more specific requirements for each position and for additional specialization within each position based upon any other skills an employee may have. The job descriptions for each position are descriptive but remain fairly broad because of the nature of the work for which each position is responsible. The employee understands that there are general skills that people within their given role must have and that the job description augments those skills.

Management's Philosophy and Operating Style

Shapco management philosophy and operating style is ultimately responsible for the system of internal controls. Virtually all employees have some role in controlling the organization. Some controls are established at the organization level, and management of the local unit establishes others. Management has formal policies and procedures in place to guide personnel on specific information processing functions.

Organizational Structure

Management has designed the organizational structure to provide quality service and accountability in support of Shapco's mission. In order to achieve quality in performance, they strive for continuous improvement in all that is done, plan and commit to accomplish targets, and are empowered to perform their duties. Shapco's operations are highly specialized and require the ability to adapt to industry changes and best practices. Shapco has a centralized, flat management framework, which allows them to quickly react to industry changes and have excellent response times to client needs. In addition, the CEO / President is an active participant in day-to-day operations and managers report directly to him. An organizational chart is in place to communicate key areas of authority, responsibility, and appropriate lines of reporting to personnel. These charts are available to personnel via the intranet.

Human Resource Policies and Practices

Shapco's human resource policies and practices are clearly written and communicated where appropriate. Policies and procedures that are listed in the employee handbook include hiring, training, disciplinary actions and termination procedures.

Risk Assessment

Risk assessment is the process of identifying and analyzing relevant risks which, if realized, could prevent Shapco from achieving its operational compliance objectives. Shapco assesses and manages risks that could affect the organization's ability to provide services to its clients on an ongoing basis. For any significant risks identified, management is responsible for implementing appropriate measures to remediate or manage these risks (e.g., implementing / revising control procedures, conducting specific audit projects, designing, and delivering issue-specific training).

The executive management team, as part of its annual information security policy review, considers developments in technology and the impact of applicable laws and regulations on Shapco's security policies.

Changes in security threats and risks are reviewed by Shapco management and updates to existing control activities and information security policies are performed as necessary.

Shapco management maintains a series of tools for the monitoring and management of:

- Severe weather / Natural Disasters
- Infrastructure failures
- Unauthorized intrusion; logical and physical
- Vendor failures
- Criminal activity
- Compromise of production equipment
- Loss of key employee personnel
- Data protection and datacenter protection

The aforementioned list comprises the tools for monitoring and management support of Shapco's communications network, servers, applications, security, and devices utilized in Shapco's overall operation for providing business process services.

Information and Communication Systems

Information System

Shapco has and maintains an information security policy to help ensure that employees understand their individual roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time sensitive information and processes for security and system availability purposes that notify key personnel in the event of potential security issues or system outages.

Communication System

Shapco utilizes various methods of communication to help ensure:

- Employees understand their individual roles and responsibilities and company controls
- Those significant events are communicated in a timely manner

Time sensitive information is communicated verbally and via email to employees and contractors. Management holds regular staff meetings as an additional forum for communications. Furthermore, employees receive written job descriptions that clearly define their roles, responsibilities, and expectations within the organization.

Monitoring

On-Going Monitoring

Shapco's management performs monitoring activities in order to assess the quality of internal control over time and monitors activities throughout the year and takes corrective actions to address deviations from company policy and procedures. Management utilizes a risk-based approach to monitor business units and other auditable entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed in order of significance.

Shapco monitors client communications through email and allocated Shapco client management personnel. This information is reviewed by management the ability to track, monitor, and assist in understanding client complaints, concerns, and to evaluate and resolve special requests in a timely fashion. Management's ability to actively monitor client's communications is an integral role in controlling the quality of the services provided.

Management is proactive in responding to client complaints and there is a high level of inter-departmental communication about these events. Client complaints and other issues are handled immediately via an internal ticketing system and by personal contact by management staff. Major client-facing issues are immediately reported to the CEO / President for discussion and approval of action.

Policies and Practices

INFRASTRUCTURE MANAGEMENT

Shapco is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Printing, Mailing, and Fulfillment Services system. These controls provide the basis for reliance on information / data from the systems used by user entities.

Physical and Environmental Security

The Controller is responsible for validating that physical access authority defined within the system is in alignment with assigned job responsibilities. In addition, card keys maintained by employees are reviewed periodically to ensure serial numbers on the key cards match information maintained within the security system for each employee. Production application and file servers critical to operations are located within a locked data center within the facility. Data center access is limited to members of the IT and Management.

Access to the Shapco facility requires a valid key card that has been approved and distributed by the Controller. Access to areas within Shapco is based on the profile of the key fob as defined in the profile definition matrix. The profile defines day and time of day access for each role and can be either limited or 24-hour access. Key fobs are then provisioned to Shapco employees in accordance to the profile definition matrix.

The Shapco data center is equipped with an inert gas fire suppression system, an independent air conditioning system with a backup, and an uninterruptable battery backup power (UPS).

The inert gas fire suppression system is tested annually by a professional third-party. The UPS is tested on a monthly basis and batteries within the unit are replaced on an annual basis. The air conditioning system is monitored on an ongoing basis with an audible alert generated if the established threshold is exceeded.

In addition, Shapco has fire extinguishers placed in locations throughout the facility as required by local fire code which are tested annually by an outside vendor.

Change Management

Shapco has a formal change management process in place which requires identification and recording of significant changes, assessment of risk and potential effect of such changes, approval of proposed changes, and testing of changes to verify operational functionality. Proposed changes are evaluated to determine if they present a security risk and what mitigating actions, including employee and user entity notifications, must be performed. The IT management team meets weekly to review and schedule changes to the IT environment.

Emergency changes follow the formalized change management process, but at an accelerated timeline. Prior to initiating an emergency change, necessary approvals are obtained and documented.

Changes to infrastructure are tested prior to implementation.

Software at Shapco is purchased and therefore no internal development is performed. Software updates and patches are tested prior to implementation into the production environment.

System Monitoring

Commercially available monitoring software (SolarWinds) is used to monitor the performance of the Microsoft Windows production servers and is administered by Shapco. This software monitors the current status of the servers. Performance counters that are monitored include but are not limited to:

- CPU utilization
- Memory utilization
- Disk utilization
- System availability

Alerts are generated when performance counter thresholds have been exceeded. The alerts are sent out via email to respective mailboxes which are monitored by the IT team.

Shapco maintains a network security appliance (an intrusion prevention system – IPS) that monitors its network for potential intuitions, hacking signatures, and malicious activity. The function of the IPS is to identify potential malicious activity, log information about the activity, attempt to block and stop the activity, and report the activity to management for further investigation.

Problem Management

Security incidents and other IT-related problems are reported to the help desk and IT management and resolved as best determined appropriate.

Data Backup and Recovery

Shapco performs disk-to-disk (interim step to tape) backup activities to support data storage and recovery objectives. Symantec Backup Exec software is used to manage data backup activities.

On a periodic basis, the IT Manager restores data from the off-site storage system to ensure data recovery in the event of a long-term service disruption. At the end of the business day, a full backup is run and transferred to an online backup system that is external to Shapco and in excess of seven miles from the Shapco facility.

Logical Security

Shapco has implemented role-based security to limit and control access within its applications. Employees are granted logical and physical access to in-scope systems based on documented approvals by appropriate management personnel. Server administrator privileges are assigned to designated employees within Shapco. In addition, local administrator accounts have been established on servers to perform software maintenance activities.

Logical access to network resources and application systems are based on business need. Permissions are established based on the defined responsibilities of the role assigned to the employee. Shapco has established structured procedures for adding, changing, and deleting user accounts.

The Controller is responsible for overseeing the employee separation process for personnel that are leaving the organization either voluntarily or involuntarily and for completing an Add, Change, Delete Form that identifies the systems that user's access should be disabled or deleted. Notification of termination is forwarded to the IT Manager for user account processing. This process includes disabling and deleting user accounts. Situations that require immediate dismissal of staff may be communicated verbally and followed by appropriate written documentation.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

The principles, criteria, and related controls are included in Section 4 of this report, “Principles, Criteria, Related Controls and Tests of Operating Effectiveness”, to eliminate the redundancy that would result from listing them in this section and repeating them in Section 4. Although the principles and related controls are included in Section 4, they are, nevertheless, an integral part of the organization’s description of controls.

COMPLEMENTARY CONTROL CONSIDERATIONS

Shapco's policies and procedures over its Printing, Mailing, and Fulfillment Services system cover only a portion of the overall internal control for each user entity. It is not feasible for the principles and criteria related to the Printing, Mailing, and Fulfillment Services system to be solely achieved by Shapco. Shapco's control policies and procedures were designed with the assumption that certain controls would be in place and in operation at the user entities. User entity internal controls must be evaluated, taking into consideration Shapco controls and their own internal controls. Shapco management does not make any representations regarding responsibility related to or provide any assurance in regard to any such internal control or regulatory requirements for which the client must assess or comply.

This section describes some of the control considerations for user entities, or "complementary controls", which should be in operation at the user entities to complement the controls at the service organization. User auditors / user entities should determine whether user entities have established controls to ensure that the criteria within this report are met. The "complementary controls" presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities.

Control Considerations for User Entities

1. User entities are responsible for sending data files via a secure connection.
2. User entities are responsible for encrypting data files that cannot be transmitted via a secure connection.
3. User entities are responsible for communicating and reporting the total document and page counts.
4. User entities are responsible for communicating and reporting file names transmitted.
5. User entities are responsible for communicating and reporting mailing counts and / or postage costs.
6. User entities are responsible for communicating and reporting any other detail that can be used as a "checks and balances" measure in confirming accuracy and completeness.
7. User entities are responsible for performing timely additions and / or removals of their users from access to the Storefront website.
8. User entities are responsible for the ensuring user IDs are not shared for accessing the Storefront website.
9. User entities are responsible for the approval of the orders submitted via the Storefront website.
10. User entities are responsible for complete, accurate, and timely review of proofs supplied by Shapco.

SECTION 4:

PRINCIPLES, CRITERIA, CONTROL DESCRIPTIONS, RELATED CONTROLS AND TESTS OF OPERATING EFFECTIVENESS

INFORMATION PROVIDED BY THE SERVICE AUDITOR

Introduction

This report is intended to provide user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding with information about controls that may affect the Printing, Mailing, and Fulfillment Services system provided by Shapco and to provide information about the operating effectiveness of controls that were tested.

The scope of our testing of Shapco's controls was limited to the principles, criteria, and the related controls specified by Shapco and contained within Section 4 of this report, which management believes to be the relevant key controls for the principles and criteria included in the scope of this report.

The examination was performed in accordance with the American Institute of Certified Public Accountants ("AICPA") Standards for Attestation Engagements No. 18 '*Attestation Standards: Clarification and Recodification*', specifically AT-C Section 105, "*Concepts Common to All Attestation Engagements*' and AT-C Section 205, '*Examination Engagements*.' It is each interested party's responsibility to evaluate this information in relation to controls in place at user entities and sub-service organizations (if applicable) to obtain an overall understanding of internal control and to assess control risk. Controls in place at user entities, sub-service organizations (if applicable), and Shapco's controls must be evaluated together. A general, but not inclusive, listing of control considerations is provided in Section 3, "Complementary Control Considerations." If an effectively operating user entity or sub-service organization (if applicable) internal control is not in place, the controls at Shapco may not sufficiently compensate the deficiency.

Tests of Operating Effectiveness

Our tests of the operating effectiveness of the controls specified by Shapco included such tests as we considered necessary in the circumstances to obtain reasonable, but not absolute, assurance that the controls operated in a manner that achieved the specified principle during the period from May 16, 2017 to April 30, 2018. In selecting particular tests of the operating effectiveness of controls we considered 1) the nature of the controls being tested; 2) the types and completeness of available evidential matter; 3) the nature of the principle to be achieved; 4) the assessed level of control risk; 5) the expected efficiency and effectiveness of the test; and, 6) the testing of other controls relevant to the principle.

Testing exceptions, if any, and information about specific tests of the operating effectiveness performed that may be relevant to the interpretation of testing results by user entities, prospective user entities, independent auditors and practitioners providing services to such user entities, and regulators who have sufficient knowledge and understanding for the controls specified to achieve the principle are presented in this section under the column heading "Results of Testing". Exceptions identified herein are not necessarily considered significant deficiencies or material weaknesses in the total system of internal controls of Shapco, as this determination can only be made after consideration of controls in place at user entities. Control considerations that should be exercised by Shapco's clients in order to complement the controls of Shapco to attain the principles are presented in relation to the nature of services being audited and the controls specified by Shapco.

Types of Tests Performed

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

Test Types	Description of Tests
Inquiry	Inquired of appropriate personnel seeking relevant information or representation to obtain the following information about the control: ➢ Knowledge and additional information regarding the policy or procedure ➢ Corroborating evidence of the policy or procedure
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: ➢ Examination / Inspection of source documentation and authorizations to verify transactions processed ➢ Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures ➢ Examination / Inspection of systems documentation, configurations and settings ➢ Examination / Inspection of procedural documentation such as operations manuals, flow charts and job descriptions
Observation	Observed the implementation, application or existence of specific controls as represented
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed

Sampling Methodology

The table below describes the sampling methodology utilized in our testing to evaluate the operational effectiveness of the controls detailed in the matrices that follow:

Type of Control and Frequency	Minimum Number of Items to Test (Period of Review Six Months or Less)	Minimum Number of Items to Test (Period of Review More than Six Months)
Manual control, many times per day	At least 25	At least 40
Manual control, daily (Note 1)	At least 25	At least 40
Manual control, weekly	At least 5	At least 10
Manual control, monthly	At least 3	At least 4
Manual control, quarterly	At least 2	At least 2
Manual control, annually	Test annually	Test annually
Application controls	Test one operation of each relevant aspect of each application control if supported by effective IT general controls; otherwise test at least 15	Test one operation of each application control if supported by effective IT general controls; otherwise test at least 25
IT general controls	Follow guidance above for manual and automated aspects of IT general controls	Follow guidance above for manual and automated aspects of IT general controls

Notes: 1.) Some controls might be performed frequently, but less than daily. For such controls, the sample size should be interpolated using the above guidance. Generally, for controls where the number of occurrences ranges from 50 to 250 during the year, our minimum sample size using the above table should be approximately 10% of the number of occurrences.

PRINCIPLES, CRITERIA, AND RELATED CONTROLS

Security Principle and Criteria (Common Criteria to All Principles)

The system is protected against unauthorized access, use, or modification to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC1.0 Organization and Management: The criteria relevant to how the organization is structured and the processes the entity has implemented to manage and support people within its operating units to meet the criteria for the principles addressed by the engagement. This includes criteria addressing accountability, integrity, ethical values and qualifications of personnel, and the environment in which they function.			
CC1.1 The entity has defined organizational structures, reporting lines, authorities, and responsibilities for the design, development, implementation, maintenance operation, and monitoring of the system enabling it to meet its commitments and system requirements as they relate to security, availability, and confidentiality.			
CC1.1.1	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.
CC1.1.2	Organizational charts are in place to communicate areas of authority, responsibility, and the lines of reporting to personnel. These charts are available to personnel via the intranet.	Inquired of the Controller to verify that organizational charts were in place to communicate areas of authority, responsibility, and the lines of reporting to personnel and these charts were available to personnel via the intranet.	No relevant exceptions noted.
		Inspected the organizational chart and its location on the company intranet to verify that organizational charts were in place to communicate areas of authority, responsibility, and the lines of reporting to personnel and these charts were available to personnel via the intranet.	No relevant exceptions noted.
CC1.1.3	Management has assigned ownership of the policies and procedures to the various department leaders.	Inquired of the Controller to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Shapco policies ownership document to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC1.2.1	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.
CC1.2.2	Organizational charts are in place to communicate areas of authority, responsibility, and the lines of reporting to personnel. These charts are available to personnel via the intranet.	Inquired of the Controller to verify that organizational charts were in place to communicate areas of authority, responsibility, and the lines of reporting to personnel and these charts were available to personnel via the intranet.	No relevant exceptions noted.
		Inspected the organizational chart and its location on the company intranet to verify that organizational charts were in place to communicate areas of authority, responsibility, and the lines of reporting to personnel and these charts were available to personnel via the intranet.	No relevant exceptions noted.
CC1.2.3	Management has assigned ownership of the policies and procedures to the various department leaders.	Inquired of the Controller to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.
		Inspected the Shapco policies ownership document to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing 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, availability, and confidentiality and provides resources necessary for personnel to fulfill their responsibilities.			
CC1.3.1	Employee candidates' ability to meet job requirements is evaluated as part of the hiring evaluation process.	Inquired of the Controller to verify that employee candidates' ability to meet job requirements was evaluated as part of the hiring evaluation process.	No relevant exceptions noted.
		Inspected New Hire Checklists for indication of review of the candidates' ability to perform job responsibilities for a sample of new hires on-boarded during the examination period to verify that employee candidates' ability to meet job requirements were evaluated as part of the hiring evaluation process.	No relevant exceptions noted.
CC1.3.2	Management maintains policy and procedure documents on the company intranet.	Inquired of the Controller to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC1.4.1	As part of the on-boarding process, new employees are required to sign to a statement indicating that they have read, understand, and will follow the Employee Handbook and the company policy and procedures.	Inquired of the Controller to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the signed employee handbook receipt / acknowledgment forms for a sample of employees on-boarded during the examination period to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
CC1.4.2	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
CC1.4.3	Management performs criminal background checks on new employees prior to on-boarding.	Inquired of the Controller to verify that management performed criminal background checks on new employees prior to on-boarding.	No relevant exceptions noted.
		Inspected the results of background screenings performed for a sample of employees on-boarded during the examination period to verify that management performed criminal background checks on new employees prior to on-boarding.	No relevant exceptions noted.
CC2.0 Communications: The criteria relevant to how the organization communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and uses to the effective operation of the system.			
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 to permit users to understand their role in the system and the results of system operation.			
CC2.1.1	A login banner is displayed prior to login to the network for internal users. The banner explains that the content of the workstation is the property of Shapco and unauthorized use is prohibited.	Inquired of the Controller to verify that a login banner was displayed prior to login to the network for internal users and the banner explained that the content of the workstation was the property of Shapco and unauthorized use was prohibited.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the login banner on an example of a Shapco system to verify that a login banner was displayed prior to login to the network for internal users and the banner explained that the content of the workstation was the property of Shapco and unauthorized use was prohibited.	No relevant exceptions noted.
CC2.1.2	As part of the on-boarding process, new employees are required to sign to a statement indicating that they have read, understand, and will follow the Employee Handbook and the company policy and procedures.	Inquired of the Controller to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
		Inspected the signed employee handbook receipt / acknowledgment forms for a sample of employees on-boarded during the examination period to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
CC2.1.3	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.
CC2.1.4	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.1.5	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
CC2.1.6	Management maintains policy and procedure documents on the company intranet.	Inquired of the Controller to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
CC2.2 The entity's security, availability, and confidentiality 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.			
CC2.2.1	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
CC2.2.2	Employees with credentials that allow access to systems are required to complete the company security training annually.	Inquired of the Controller to verify that employees with credentials that allowed access to systems were required to complete the company security training annually.	No relevant exceptions noted.
		Inspected the training completion results for a sample of active employees within the examination period to verify that employees with credentials that allowed access to systems were required to complete the company security training within the past 12 months.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.2.3	As part of the on-boarding process, new employees are required to sign to a statement indicating that they have read, understand, and will follow the Employee Handbook and the company policy and procedures.	Inquired of the Controller to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
		Inspected the signed employee handbook receipt / acknowledgment forms for a sample of employees on-boarded during the examination period to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
CC2.3 The responsibility of internal and external users and other whose roles affect system operation are communicated to those parties.			
CC2.3.1	As part of the on-boarding process, new employees are required to sign to a statement indicating that they have read, understand, and will follow the Employee Handbook and the company policy and procedures.	Inquired of the Controller to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
		Inspected the signed employee handbook receipt / acknowledgment forms for a sample of employees on-boarded during the examination period to verify that as part of the on-boarding process, new employees were required to sign to a statement indicating that they had read, understood, and would follow the Employee Handbook and the company policy and procedures.	No relevant exceptions noted.
CC2.3.2	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.3.3	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
CC2.3.4	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
CC2.4 Information necessary for designing, developing, implementing, operating, maintaining, and monitoring controls, relevant to the security, availability, and confidentiality of the system, is provided to personnel to carry out their responsibilities.			
CC2.4.1	Management maintains policy and procedure documents on the company intranet.	Inquired of the Controller to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that management maintained policy and procedure documents on the company intranet.	No relevant exceptions noted.
CC2.4.2	Roles and responsibilities are defined in written job descriptions.	Inquired of the Controller to verify that roles and responsibilities were defined in written job descriptions.	No relevant exceptions noted.
		Inspected the documented job descriptions to verify that roles and responsibilities for key positions were defined in written job descriptions.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC2.4.3	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
CC2.5 Internal and external users have been provided with information on how to report security, availability, and confidentiality failures, incidents, concerns, and other complaints to appropriate personnel.			
CC2.5.1	Customers are assigned a Shapco representative who is charged with overseeing work performed and act as the point-of-contact.	Inquired of the Controller to verify that customers were assigned a Shapco representative who was charged with overseeing work performed and acted as the point-of-contact.	No relevant exceptions noted.
		Inspected the customer contact listing of representatives to verify that customers were assigned a Shapco representative who was charged with overseeing work performed and acted as the point-of-contact.	No relevant exceptions noted.
CC2.5.2	Employees with credentials that allow access to systems are required to complete the company security training annually.	Inquired of the Controller to verify that employees with credentials that allowed access to systems were required to complete the company security training annually.	No relevant exceptions noted.
		Inspected the training completion results for a sample of active employees within the examination period to verify that employees with credentials that allowed access to systems were required to complete the company security training within the past 12 months.	No relevant exceptions noted.
CC2.5.3	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
CC2.5.4	Management has documented and maintains an Incident Response Policy on the company Intranet.	Inquired of the Controller to verify that management had documented and maintained an Incident Response Policy on the company Intranet.	No relevant exceptions noted.
		Inspected the Incident Response Policy and its location on the company intranet to verify that management had documented and maintained an Incident Response Policy on the company intranet.	No relevant exceptions noted.
CC2.5.5	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
		Inspected the security reminder emails sent out to employees for a sample of quarters within the examination period to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
CC2.6 System changes that affect internal and external users' responsibilities or the entity's commitments and system requirements relevant to security, availability, and confidentiality are communicated to those users in a timely manner.			
CC2.6.1	Customers are assigned a Shapco representative who is charged with overseeing work performed and act as the point-of-contact.	Inquired of the Controller to verify that customers were assigned a Shapco representative who was charged with overseeing work performed and acted as the point-of-contact.	No relevant exceptions noted.
		Inspected the customer contact listing of representatives to verify that customers were assigned a Shapco representative who was charged with overseeing work performed and acted as the point-of-contact.	No relevant exceptions noted.
CC2.6.2	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the security reminder emails sent out to employees for a sample of quarters within the examination period to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
CC3.0 Risk Management and Design and Implementation of Controls: The criteria relevant to how the entity (i) identifies potential risks that would affect the entity's ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.			
CC3.1 The entity (1) identifies potential threats that could impair system security, availability, and confidentiality 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 other with access to the system), (2) analyzes the significance of risks associated with the identified threats, and (3) determines mitigation strategies for those risks (including implementation of controls, assessment and monitoring of vendors and other third parties providing goods and 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.			
CC3.1.1	Management maintains an inventory of the Shapco system components.	Inquired of the VP of Technologies to verify that management maintained an inventory the Shapco system components.	No relevant exceptions noted.
		Inspected the inventory listing to verify that management maintained an inventory of the Shapco system components.	No relevant exceptions noted.
CC3.1.2	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.1.3	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	Inquired of the VP of Technologies to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	No relevant exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	No relevant exceptions noted.
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.			
CC3.2.1	Policies and procedures regarding Security, Availability, and Confidentiality are documented and available to guide personnel.	Inquired of the Controller and VP of Technologies to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
		Inspected the policies and procedures and their location on the company intranet to verify that policies and procedures regarding Security, Availability, and Confidentiality were documented and available to guide personnel.	No relevant exceptions noted.
CC3.2.2	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC3.2.3	A business continuity plan is in place and reviewed annually by management.	Inquired of the VP of Technologies to verify that a business continuity plan was in place and reviewed annually by management.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan was in place and reviewed within the past 12 months by management.	No relevant exceptions noted.
CC3.2.4	A risk assessment is performed annually and includes identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	Inquired of the VP of Technologies to verify that a risk assessment was performed annually and included identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	No relevant exceptions noted.
		Inspected the most recent risk assessment to verify that a risk assessment was performed within the past 12 months and included identifying and assessing the risks associated with identified threats that may impair system security, availability, and confidentiality.	No relevant exceptions noted.
CC4.0 Monitoring Controls: The criteria relevant to how the entity monitors the system, including the suitability, and design and operating effectiveness of the controls, and takes action to address deficiencies identified.			
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, availability, and confidentiality, and corrections and other necessary actions relating to identified deficiencies are taken in a timely manner.			
CC4.1.1	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC4.1.2	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
CC4.1.3	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
CC5.0 Logical and Physical Access Controls: The criteria relevant to how the organization restricts logical and physical access to the system, provides and removes that access, and prevents unauthorized access to meet the criteria for the principles addressed in the engagement.			
CC5.1 Logical access security software, infrastructure, and architectures have been implemented to support (1) identification and authentication of 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, availability, and confidentiality.			
CC5.1.1	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
CC5.1.2	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the examination period to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
CC5.1.3	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the Active Directory (AD) user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
CC5.1.4	Network authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption is disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	Inquired of the VP of Technologies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the AD policies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
CC5.1.5	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
CC5.1.6	Access to the operating systems is restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that access to the operating systems was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
		Inspected the domain administrator user listing to verify that access to the operating systems was restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
CC5.1.7	Access to the Monarch application requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Monarch user listing and password policy to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
CC5.1.8	Monarch authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	Inquired of the VP of Technologies to verify that Monarch authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	No relevant exceptions noted.
		Inspected the Monarch password and lockout policies to verify that Monarch authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	No relevant exceptions noted.
CC5.1.9	Administrative access to the Monarch application is restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that Administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the administrator user listing within the application to verify that administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
CC5.1.10	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
CC5.1.11	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
CC5.1.12	Access to the data center is restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	Inquired of the VP of Technologies to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected badge system showing users with access to the data center to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
CC5.1.13	Administrative access to the badge system is limited through a generic administrator account ID and password. Knowledge of the account credentials is limited to members of the IT team.	Inquired of the VP of Technologies to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
		Inspected physical badge access system listing the users with administrative access to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
CC5.1.14	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
CC5.1.15	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
CC5.1.16	AD and Monarch are configured to log successful and unsuccessful login attempts.	Inquired of the VP of Technologies to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
		Inspected the Eventlog Analyzer to verify that AD and Monarch were configured to log successful and unsuccessful login attempts.	No relevant exceptions noted.
CC5.1.17	AD policies are configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	Inquired of the VP of Technologies to verify that AD policies were configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	No relevant exceptions noted.
		Inspected the AD restriction policies to verify that AD policies were configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	No relevant exceptions noted.
CC5.1.18	Firewalls are in place and configured to limit traffic to the internal network.	Inquired of the VP of Technologies to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
		Inspected the firewall access rules to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
CC5.1.19	Cisco AMP is installed and configured on production servers to mitigate damage of a successful penetration of the network.	Inquired of the VP of Technologies to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected Cisco AMP running on a production server to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
CC5.1.20	On a quarterly basis, security reminders are sent out and ongoing training is performed.	Inquired of the VP of Technologies to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
		Inspected the security reminder emails sent out to employees for a sample of quarters within the examination period to verify that on a quarterly basis, security reminders were sent out and ongoing training was performed.	No relevant exceptions noted.
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, availability, and confidentiality. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			
CC5.2.1	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
CC5.2.2	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access forms and termination checklists for a sample of employees terminated within the examination period to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
CC5.2.3	The Storefront web application requires user entity employees to authenticate using user IDs and passwords.	Inquired of the VP of Technologies to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
		Inspected the Storefront application login screen to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
CC5.3 Internal and external users are identified and authenticated when accessing the system components (that is, infrastructure, software, and data) to meet the entity's commitments and system requirements as they relate to security, availability, and confidentiality.			
CC5.3.1	The Storefront web application requires user entity employees to authenticate using user IDs and passwords.	Inquired of the VP of Technologies to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
		Inspected the Storefront application login screen to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
CC5.3.2	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.3	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the examination period to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
CC5.3.4	Access to the network requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
		Inspected the AD user listing and network password policy to verify that access to the network required a unique ID and password.	No relevant exceptions noted.
CC5.3.5	Network authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption is disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	Inquired of the VP of Technologies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the AD policies to verify that network authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ complexity enabled ➢ storing passwords using reversible encryption was disabled ➢ five invalid logon attempts before lockout ➢ lockout duration 15 min	No relevant exceptions noted.
	Network Access Controls		
CC5.3.6	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
CC5.3.7	Access to the operating systems is restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that access to the operating systems was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
		Inspected the domain administrator user listing to verify that access to the operating systems was restricted to the following users: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.3.8	Access to the Monarch application requires a unique ID and password.	Inquired of the VP of Technologies to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
		Inspected the Monarch user listing and password policy to verify that access to the Monarch application required a unique ID and password.	No relevant exceptions noted.
CC5.3.9	Monarch authentication settings enforce password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	Inquired of the VP of Technologies to verify that Monarch authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	No relevant exceptions noted.
		Inspected the Monarch password and lockout policies to verify that Monarch authentication settings enforced password policies including: ➢ six character minimum passwords ➢ maximum password age 60 ➢ minimum password age 45 ➢ password history two ➢ Complexity enabled ➢ five invalid logon attempts before lockout ➢ lockout duration five minutes	No relevant exceptions noted.
CC5.3.10	Administrative access to the Monarch application is restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	Inquired of the VP of Technologies to verify that Administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the administrator user listing within the application to verify that administrative access to the Monarch application was restricted to the following personnel: ➢ VP of Technologies ➢ Contractor (2)	No relevant exceptions noted.
CC5.3.11	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC5.4.1	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
CC5.4.2	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
CC5.4.3	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the examination period to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC5.5.1	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
CC5.5.2	Access to the data center is restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	Inquired of the VP of Technologies to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected badge system showing users with access to the data center to verify that access to the data center was restricted to the following personnel: ➢ VP of Technologies ➢ Pre-press Manager ➢ Pre-press Tech (2)	No relevant exceptions noted.
CC5.5.3	Administrative access to the badge system is limited through a generic administrator account ID and password. Knowledge of the account credentials is limited to members of the IT team.	Inquired of the VP of Technologies to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
		Inspected physical badge access system listing the users with administrative access to verify that administrative access to the badge system was limited through a generic administrator account ID and password and knowledge of the account credentials was limited to members of the IT team.	No relevant exceptions noted.
CC5.5.4	Visitors are required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	Inquired of the VP of Technologies and of the receptionist to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Observed the requirements to sign into a guest log, wear a badge, and be escorted during the onsite walk-throughs of the facility to verify that visitors were required to sign into a guest log, wear a visitor ID, and be escorted during onsite.	No relevant exceptions noted.
		Inspected the visitor logs for the examination period to verify that visitors were required to sign into a guest log.	No relevant exceptions noted.
CC5.5.5	Perimeter doors are locked with the exception of the main entrance which is staffed during office hours. After hours, the main entrance is also locked.	Inquired of the VP of Technologies to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the perimeter doors during onsite walk-throughs to verify that perimeter doors were locked with the exception of the main entrance which was staffed during office hours and after hours, the main entrance was also locked.	No relevant exceptions noted.
CC5.5.6	Video surveillance systems are in place throughout the facility, including the data center, and are configured to record and maintain footage for a minimum of 30 days.	Inquired of the VP of Technologies to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
		Inspected the video surveillance system and footage to verify that video surveillance systems were in place throughout the facility, including the data center, and were configured to record and maintain footage for a minimum of 30 days.	No relevant exceptions noted.
CC5.5.7	The badge access system logs and maintains activity for 30 days prior to being backed up.	Inquired of the VP of Technologies to verify that the badge access system logged and maintained activity for 30 days prior to being backed up.	No relevant exceptions noted.
		Inspected the badge access system and example logs to verify that the badge access system logged and maintained activity for activity for 30 days prior to being backed up.	No relevant exceptions noted.
CC5.5.8	Printed materials waiting to be shipped out are maintained within a secure location.	Inquired of the VP of Technologies to verify that printed materials, including mailings, waiting to be shipped out were maintained within a secure location.	No relevant exceptions noted.
		Observed the secure location utilized to store confidential printed materials prior to being shipped to verify that printed materials, including mailings, waiting to be shipped out were maintained within a secure location.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.6 Logical access security measures have been implemented to protect against security, availability, and confidentiality threats from sources outside the boundaries of the system to meet the entity's commitments and system requirements.			
CC5.6.1	Firewalls are in place and configured to limit traffic to the internal network.	Inquired of the VP of Technologies to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
		Inspected the firewall access rules to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
CC5.6.2	Administrative access to the firewall system is limited to the members of the IT department.	Inquired of the VP of Technologies to verify that administrative access to the firewall system was limited to the members of the IT department.	No relevant exceptions noted.
		Inspected the firewall administrator user listing to verify that administrative access to the firewall system was limited to the members of the IT department.	No relevant exceptions noted.
CC5.6.3	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
CC5.6.4	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.6.5	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
CC5.6.6	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC5.7.1	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
CC5.7.2	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
CC5.7.3	Logical and physical access assigned to terminated employees is deactivated, disabled, or assigned a new password at the time of termination.	Inquired of the VP of Technologies to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
		Inspected the access forms and termination checklists for a sample of employees terminated within the examination period to verify that logical and physical access assigned to terminated employees was deactivated, disabled, or assigned a new password at the time of termination.	No relevant exceptions noted.
CC5.7.4	An SFTP site is configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	Inquired of the VP of Technologies to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
		Inspected the configurations of the Secure FTP to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
CC5.7.5	AD policies are configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	Inquired of the VP of Technologies to verify that AD policies were configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	No relevant exceptions noted.
		Inspected the AD restriction policies to verify that AD policies were configured to restrict installation of applications and use of drives and USB ports for computers on the domain.	No relevant exceptions noted.
CC5.7.6	The Storefront web application requires user entity employees to authenticate using user IDs and passwords.	Inquired of the VP of Technologies to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Storefront application login screen to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
CC5.7.7	The Storefront web application utilizes TLS encryption to secure customer transactions.	Inquired of the VP of Technologies to verify that the Storefront web application utilized TLS encryption to secure customer transactions.	No relevant exceptions noted.
		Inspected the web certificate for the Storefront web application to verify that the Storefront web application utilized TLS encryption to secure customer transactions.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC5.8.1	A centralized anti-virus system is in place to monitor anti-virus installations and configurations on the production workstations and servers.	Inquired of the VP of Technologies to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.
		Inspected the Symantec Endpoint Protection Manager system and Cisco AMP system to verify that a centralized anti-virus system was in place to monitor anti-virus installations and configurations on the production workstations and servers.	No relevant exceptions noted.
CC5.8.2	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC5.8.3	Cisco AMP is installed and configured on production servers to mitigate damage of a successful penetration of the network.	Inquired of the VP of Technologies to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
		Inspected Cisco AMP running on a production server to verify that Cisco AMP was installed and configured on production servers to mitigate damage of a successful penetration of the network.	No relevant exceptions noted.
CC5.8.4	Firewalls are in place and configured to limit traffic to the internal network.	Inquired of the VP of Technologies to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
		Inspected the firewall access rules to verify that firewalls were in place and configured to limit traffic to the internal network.	No relevant exceptions noted.
CC6.0 System Operations: The criteria relevant to how the organization manages the execution of system procedures and detects and mitigates processing deviations, including logical and physical security deviations, to meet the objectives of the principles addressed in the engagement.			
CC6.1 Vulnerabilities of system components to security, availability, and confidentiality 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, availability, and confidentiality.			
CC6.1.1	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
CC6.1.2	WSUS is configured and utilized to apply monthly patches to Windows workstations and servers.	Inquired of the VP of Technologies to verify that WSUS was configured and utilized to apply monthly patches to Windows workstations and servers.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the completed WSUS patching for a sample of months within the examination period to verify that WSUS was configured and utilized to apply monthly patches to Windows workstations and servers.	No relevant exceptions noted.
CC6.1.3	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
CC6.2 security, availability, and confidentiality 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.			
CC6.2.1	Management has documented and maintains an Incident Response Policy on the company Intranet.	Inquired of the Controller to verify that management had documented and maintained an Incident Response Policy on the company Intranet.	No relevant exceptions noted.
		Inspected the Incident Response Policy and its location on the company intranet to verify that management had documented and maintained an Incident Response Policy on the company intranet.	No relevant exceptions noted.
CC6.2.2	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.0 Change Management: The criteria relevant to how the entity identifies the need for changes to the system, makes the changes following a controlled change management process, and prevents unauthorized changes from being made to meet the criteria for the principles addressed in the engagement.			
CC7.1 The entity's commitments and system requirements, as they relate to security, availability, and confidentiality, are addressed during the system development lifecycle, including the authorization, design, acquisition, implementation, configuration, testing, modification, approval, and maintenance of system components.			
CC7.1.1	Policies related to change management practices are documented and maintained to ensure that security, availability, and confidentiality are considered when changes to the network are made.	Inquired of the VP of Technologies to verify that policies related to change management practices were documented and maintained to ensure that security, availability, and confidentiality were considered when changes to the network were made.	No relevant exceptions noted.
		Inspected the Network Hardening, Patch Management, and Software Installation policies to verify that policies related to change management practices were documented and maintained to ensure that security, availability, and confidentiality were considered when changes to the network were made.	No relevant exceptions noted.
CC7.1.2	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
CC7.1.3	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.2 Infrastructure, data, software, and procedures are updated as necessary to remain consistent with the system commitments and requirements as they relate to security, availability, and confidentiality.			
CC7.2.1	Management has assigned ownership of the policies and procedures to the various department leaders.	Inquired of the Controller to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.
		Inspected the Shapco policies ownership document to verify that management had assigned ownership of the policies and procedures to the various department leaders.	No relevant exceptions noted.
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, availability, and confidentiality.			
CC7.3.1	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
CC7.3.2	Vulnerability scans of the Shapco network are performed at minimum quarterly. Results are reviewed by management and risks identified are mitigated as determined appropriate.	Inquired of the VP of Technologies to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.
		Inspected the vulnerability scan results for a sample of quarters within the examination period to verify that vulnerability scans of the Shapco network were performed at minimum quarterly and results were reviewed by management and risks identified were mitigated as determined appropriate.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.3.3	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the examination period to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
CC7.4 Changes to system components are authorized, designed, developed, configured, documented, tested, approved, and implemented to meet the entity's security, availability, and confidentiality commitments and system requirements.			
CC7.4.1	IT management meets at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	Inquired of the VP of Technologies to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
		Inspected the Shapco Risk Assessment and Review Agenda and Minutes documentation for a sample of months within the examination period to verify that IT management met at minimum twice per month to discuss results of security events, scanning results, as well as to approve changes to the production network.	No relevant exceptions noted.
CC7.4.2	Test environments are in place that are separated from production systems.	Inquired of the VP of Technologies to verify that test environments were in place that was separated from production systems.	No relevant exceptions noted.
		Inspected the network diagrams and test environment to verify that test environments were in place that was separated from production systems.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
CC7.4.3	Administrative access to the network is restricted to members of the IT department.	Inquired of the VP of Technologies to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
		Inspected the AD Domain Administrators user listing to verify that Administrative access to the network was restricted to members of the IT department.	No relevant exceptions noted.
CC7.4.4	A ticketing system is utilized to document and track incidents and systems change requests.	Inquired of the VP of Technologies to verify that a ticketing system was utilized to document and track incidents and systems change requests.	No relevant exceptions noted.
		Inspected the ticketing system to verify that a ticketing system utilized to document and track incidents and systems change requests.	No relevant exceptions noted.

Availability Principle and Criteria

The system is available for operation and use to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing 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.			
A1.1.1	The monitoring tool is configured to monitor the health of the network and provide IT management with alerts when predefined thresholds are reached.	Inquired of the VP of Technologies to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
		Inspected the monitoring dashboard, alert configurations, and an example of an alert notification email to verify that the monitoring tool was configured to monitor the health of the network and provide IT management with alerts when predefined thresholds were reached.	No relevant exceptions noted.
A1.1.2	An IPS is in place and is configured to block suspected intrusion attempts and send alerts to IT management.	Inquired of the VP of Technologies to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant exceptions noted.
		Inspected the IPS configurations and an example alert sent to IT management to verify that an IPS was in place and was configured to block suspected intrusion attempts and send alerts to IT management.	No relevant 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.			
A1.2.1	The data center is equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	Inquired of the VP of Technologies to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Observed the environmental systems identified within the control activity within the Shapco data center to verify that the data center was equipped with the following environmental protection systems: ➢ Dedicated / secondary cooling system ➢ Battery backup ➢ Smoke detectors ➢ Inergen fire suppression system	No relevant exceptions noted.
A1.2.2	A third-party vendor inspects the fire detection and suppression systems annually to verify that the fire detection and suppression systems are in proper working order.	Inquired of the VP of Technologies to verify that a third-party vendor inspected the fire detection and suppression systems annually to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.
		Inspected the most recent third-party suppression system and fire extinguisher invoice to verify that a third-party vendor inspected the fire detection and suppression systems within the past 12 months to verify that the fire detection and suppression systems were in proper working order.	No relevant exceptions noted.
A1.2.3	The backup job schedulers are configured to perform daily backups.	Inquired of the VP of Technologies to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
		Inspected the backup job scheduler to verify that the backup job schedulers were configured to perform daily backups.	No relevant exceptions noted.
A1.2.4	The backup system provides notification of success, failure, or warning as a result of the backups performed.	Inquired of the VP of Technologies to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.
		Inspected the backup notification configurations and an example backup notification email to verify that the backup system provided notification of success, failure, or warning as a result of the backups performed.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.2.5	A business continuity plan has been documented and is in place.	Inquired of the VP of Technologies to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
		Inspected the business continuity plan to verify that a business continuity plan had been documented and was in place.	No relevant exceptions noted.
A1.2.6	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
A1.2.7	Backup policies and procedures are documented and available to guide personnel in the backup process.	Inquired of the VP of Technologies to verify that backup policies and procedures were documented and available to guide personnel in the backup process.	No relevant exceptions noted.
		Inspected the backup policy and the Shapco intranet to verify that backup policies and procedures were documented and available to guide personnel in the backup process.	No relevant exceptions noted.
A1.3 Recovery plan procedures supporting system recovery are tested to help meet the entity's availability commitments and system requirements.			
A1.3.1	On an annual basis, Shapco management reviews and updates the business continuity plans.	Inquired of the VP of Technologies to verify that, on an annual basis, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.
		Inspected the Shapco business continuity plan to verify that within the past 12 months, Shapco management reviewed and updated the business continuity plans.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
A1.3.2	On an annual basis, IT management performs a full restoration test of a virtual environment.	Inquired of the VP of Technologies to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.
		Inspected an example of a backup restoration test to verify that within the past 12 months, IT management performed a full restoration test of a virtual environment.	No relevant exceptions noted.

Confidentiality Principle and Criteria

Information designated as confidential is protected to meet the entity's commitments and system requirements.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.1 Confidential information is protected during the system design, development, testing, implementation, and change processes to meet the entity's confidentiality commitments and system requirements.			
C1.1.1	On an annual basis, management reviews and updates the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy. These policies are maintained on the company intranet.	Inquired of the VP of Technologies to verify that within the past 12 months, management reviewed and updated the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and these policies were maintained on the company intranet.	No relevant exceptions noted.
		Inspected the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and their location on the intranet to verify that within the past 12 months, management reviewed and updated the Software Installation Policy, the Data Classification Policy, and the Data Transmission Policy and these policies were maintained on the company intranet.	No relevant exceptions noted.
C1.1.2	Management has configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	Inquired of the VP of Technologies to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
		Inspected the AD, Monarch, and badge access systems to verify that Management had configured groups with role-based privileges within AD, Monarch, and the physical badge access system.	No relevant exceptions noted.
C1.1.3	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
C1.2 Confidential information within the boundaries of the system is protected against unauthorized access, use, and disclosure during input, processing, retention, output, and disposition to meet the entity's confidentiality commitments and system requirements.			
C1.2.1	Logical and physical access privileges are approved by management during new hire employee on-boarding.	Inquired of the VP of Technologies to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
		Inspected the access forms for a sample of employees that were on-boarded during the examination period to verify that logical and physical access privileges were approved by management during new hire employee on-boarding.	No relevant exceptions noted.
C1.2.2	Access to the production database is restricted to the Domain Administrators and requires the use of a unique ID and password.	Inquired of the VP of Technologies to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
		Inspected the SQL user listing to verify that access to the production database was restricted to the Domain Administrators and required the use of a unique ID and password.	No relevant exceptions noted.
C1.2.3	Printed materials waiting to be shipped out are maintained within a secure location.	Inquired of the VP of Technologies to verify that printed materials, including mailings, waiting to be shipped out were maintained within a secure location.	No relevant exceptions noted.
		Observed the secure location utilized to store confidential printed materials prior to being shipped to verify that printed materials, including mailings, waiting to be shipped out were maintained within a secure location.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.3 Access to confidential information from outside the boundaries of the system and disclosure of confidential information is restricted to authorized parties to meet the entity's confidentiality commitments and system requirements.			
C1.3.1	Access to the internal network from outside of the facility is limited through VPN protocols configured to authenticate with the AD.	Inquired of the VP of Technologies to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
		Inspected the VPN user access group within AD to verify that access to the internal network from outside of the facility was limited through VPN protocols configured to authenticate with the AD.	No relevant exceptions noted.
C1.3.2	An SFTP site is configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	Inquired of the VP of Technologies to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
		Inspected the configurations of the Secure FTP to verify that an SFTP site was configured and utilized by Shapco to provide options for secure uploading of customer information directly to Shapco.	No relevant exceptions noted.
C1.3.3	A confidentiality disclaimer is contained within corporate emails.	Inquired of the VP of Technologies to verify that a confidentiality disclaimer was contained within corporate emails.	No relevant exceptions noted.
		Inspected an example of a Shapco email to verify that a confidentiality disclaimer was contained within corporate emails.	No relevant exceptions noted.
C1.3.4	The Storefront web application requires user entity employees to authenticate using user IDs and passwords.	Inquired of the VP of Technologies to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.
		Inspected the Storefront application login screen to verify that the Storefront web application required user entity employees to authenticate using user IDs and passwords.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
C1.3.5	The Storefront web application utilizes TLS encryption to secure customer transactions.	Inquired of the VP of Technologies to verify that the Storefront web application utilized TLS encryption to secure customer transactions.	No relevant exceptions noted.
		Inspected the web certificate for the Storefront web application to verify that the Storefront web application utilized TLS encryption to secure customer transactions.	No relevant exceptions noted.
C1.4 The entity obtains confidentiality commitments that are consistent with the entity's confidentiality requirements from vendors and other third parties whose products and services are part of the system and have access to confidential information.			
C1.4.1	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
C1.5 Compliance with the entity's confidentiality commitments and system requirements by vendors and others third parties whose products and services are part of the system is assessed on a periodic and as-needed basis, and corrective action is taken, if necessary.			
C1.5.1	Management obtains signatures from contractors indicating they have read and will adhere to Shapco Security Policies prior to access being provided.	Inquired of the Controller to verify that management obtained signatures from contractors indicating they had read and would adhere to Shapco Security Policies prior to access being provided.	No relevant exceptions noted.
		No tests of the control were performed because the circumstances that warranted the operation of the control did not occur during the examination period.	N/A
C1.6 Changes to the entity's confidentiality commitments and system requirements are communicated to internal and external users, vendors, and other third parties whose products and services are part of the system.			
C1.6.1	Shapco maintains its Terms of Use and Privacy statements on the company website for external users.	Inquired of the Controller to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.

#	Control Activities Specified by the Service Organization	Tests Applied by the Service Auditor	Testing Results
		Inspected the Terms of Use and Privacy statements on the company website to verify that Shapco maintained its Terms of Use and Privacy statements on the company website for external users.	No relevant exceptions noted.
C1.7 The entity retains confidential information to meet the entity's confidentiality commitments and system requirements.			
C1.7.1	The data retention policy outlines the retention periods and procedures for the protection of assets and covered information.	Inquired of the VP of Technologies to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
		Inspected the Retention Policy to verify that to verify that the data retention policy outlined the retention periods and procedures for the protection of assets and covered information.	No relevant exceptions noted.
C1.8 The entity disposes of confidential information to meet the entity's confidentiality commitments and system requirements.			
C1.8.1	A third-party vendor is utilized to perform onsite shredding of documentation designated as confidential data after the retention period has expired.	Inquired of the VP of Technologies to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
		Observed the shred bin located within the Shapco facility during onsite walkthroughs to verify that a third-party vendor was utilized to perform onsite shredding of documentation designated as confidential data after that retention period had expired.	No relevant exceptions noted.
C1.8.2	A Destruction Declaration is retained as evidence of the destruction of documentation.	Inquired of the VP of Technologies to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.
		Inspected an example of a recent destruction declaration to verify that a destruction declaration was retained as evidence of the destruction of documentation.	No relevant exceptions noted.