2012

Report on DMP's Description of its Print and Mail Production services

July 1, 2012 to December 31, 2012

Assurance Concepts
2/28/2013

DMP – SOC 1 Type II Table of Contents

To: The Management of Direct Mail Partners:

We have examined Direct Mail Partners ("DMP" or the "service organization") description of its Print and Mail Production services for high integrity receipt, printing, and mailing of user entities' documents for the period of July 1, 2012 to December 31, 2012 and the suitability of the design of controls and operating effectiveness of DMP to achieve the related control objectives stated in the description. The description indicates that certain complementary user entity controls must be suitably designed and implemented at user entities for related controls at the service organization to be considered suitably designed to achieve the related control objectives. We have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

DMP uses CoreXchange's Colocation Data Center services for their Secure File Transfer Protocol ("SFTP") server, integration website and supporting software systems (herein known as the "subservice organization"). The description of the system includes only the controls and related control objectives of DMP and does not include the control objectives and related controls of the subservice organizations. Our examination did not extend to controls of the subservice organization's Colocation Data Center services.

DMP has provided their assertion, in SECTION 2 of this report, about the fairness of the presentation of the description and suitability of the design of the controls to achieve the related controls objectives stated in the description. DMP is responsible for preparing the description and for its assertion, including the completeness, accuracy and method of presentation of the description and the assertion; providing the services covered by the description; specifying the control objectives and stating them in the description; identifying the risks that threaten the achievement of the control objectives, selecting the criteria and designing, implementing and documenting controls to achieve the related control objectives stated in the description.

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design of the controls to achieve the related control objectives stated in the description, based on our examination. We conducted our examination in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance, in all material respects, about whether the description is fairly presented and the controls were suitably designed to achieve the related control objectives stated in the description throughout the period of July 1, 2012 to December 31, 2012.

An examination of a description of a service organization's system and the suitability of the design of the service organization's controls to achieve the related control objectives stated in the description involves performing procedures to obtain evidence about the fairness of the presentation of the description of the system and the suitability of the design of the controls to achieve the related control objectives stated in the description. Our procedures included assessing the risks that the description is not fairly presented and that the controls were not suitably designed to achieve the related control objectives stated in the description. An examination engagement of this type also includes evaluating the overall presentation of the description and the suitability of the control objectives stated therein, and the suitability of the criteria specified by the service organization, described in management's assertion in SECTION 2 of this report. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Because of their nature, controls at a service organization or subservice organization may not prevent, or detect and correct, all errors or omissions in processing or reporting transactions. The projection to the future of any evaluation of the fairness of the presentation of the description, or any conclusions about the suitability of the design of the controls to achieve the related control objectives is subject to the risk that controls at a service organization or subservice organization may become ineffective or fail.

In our opinion, in all material respects, based on the criteria described in DMP's assertion in SECTION 2 of this report,

a. the description fairly presents the DMP Print and Mail Production services used by DMP to process transactions for its user entities of the system that were designed and implemented throughout the period July 1, 2012 to December 31, 2012.

b. the controls related to the control objectives of DMP stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period July 1, 2012 to December 31, 2012 and user entities applied the complementary user entity controls contemplated in the design of DMP's controls throughout the period July 1, 2012 to December 31, 2012.

c. the controls tested, which together with the complementary user entity controls referred to in the scope paragraph of this report, if operating effectively, were those necessary to provide reasonable assurance that the control objectives stated in the description were achieved, operated effectively throughout the period July 1, 2012 to December 31, 2012.

The specific controls tested and the nature, timing, and results of those tests are listed in SECTION 4 of the report titled "DMP's Control objectives and related controls and Independent Service Auditors Test of Controls and Results Thereof."

This report is intended solely for the information and use of DMP, user entities of DMP's Print and Mail Production services for the period of July 1, 2012 to December 31, 2012, and the independent auditors of such user entities, who have a sufficient understanding to consider it, along with other information including information about controls implemented by user entities themselves, when obtaining an understanding of user entities information and communication systems relevant to financial reporting. This report is not intended to be and should not be used by anyone other than these specified parties.

The information in section 5 of management's response to testing exceptions, "Other Information Provided by DMP" that describes DMP's response to testing exceptions noted during the audit and is presented by management of DMP to provide additional information that is not a part of DMP's Print and Mail Production services made available to user entities during the period July 1, 2012 to December 31, 2012. DMP's responses have not been subjected to the procedures applied in the examination of the description of the Print and Mail Production services and of the suitability of the design and operating effectiveness of controls to achieve the related control objectives stated in the description of the Print and Mail Production services.

Assurance Concepts, PLLC

February 28, 2013

St. Petersburg, Florida

We have prepared the description of DMP's Print and Mail Production services for user entities of the system during some or all of the period July 1, 2012 to December 31, 2012, and their user auditors who have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities of the system themselves, when assessing the risks of material misstatements of user entities' financial statements. We confirm, to the best of our knowledge and belief, that

a. the description fairly presents the Print and Mail Production services made available to user entities of the system during some or all of the period July 1, 2012 to December 31, 2012 for processing their transactions recording and reporting on their transactions. The criteria we used in making this assertion were that the description
   i. presents how the system made available to user entities of the system was designed and implemented to process relevant transactions, including
      1) the classes of transactions processed.
      2) the procedures, within both automated and manual systems, by which those transactions are initiated, authorized, recorded, processed, corrected as necessary and transferred to the reports presented to user entities of the system.
      3) how the system captures and addresses significant events and conditions, other than transactions.
      4) specified control objectives and controls designed to achieve those objectives.
      5) other aspects of our control environment, risk assessment process, information and communication systems, control activities and monitoring controls that are relevant to processing and reporting transactions of user entities of the system.
   ii. does not omit or distort information relevant to the scope of the Print and Mail Production services, while acknowledging that the description is prepared to meet the common needs of a broad range of user entities of the system and the independent auditors of those user entities and may not, therefore, include every aspect of the Print and Mail Production services that each individual user entity of the system and its auditor may consider important in its own particular environment.
b. the description includes relevant details of changes to the service organization's system.
c. the controls related to the control objectives stated in the description were suitably designed and operated effectively throughout the period July 1, 2012 to December 31, 2012 to achieve those control objectives. The criteria we used in making this assertion were that
   i. the risks that threaten the achievement of the control objectives stated in the description have been identified by the service organization;
   ii. the controls identified in the description would, if operating as described, provide reasonable assurance that those risks would not prevent the control objectives stated in the description from being achieved; and
   iii. the controls were consistently applied as designed, including whether manual controls were applied by individuals who have the appropriate competence and authority.

Direct Mail Partners

Purpose and Scope of Report

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of DMP's controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions of the user organizations' financial statement that may be affected by policies and procedures of DMP's Print and Mail Productions services.

This report describes the system and control structure of DMP as it relates to their Print and Mail Production services. It is intended to assist DMP customers and their independent auditors in determining the adequacy of the internal controls of services that are outsourced to DMP and are relevant to customers' internal control structures as it relates to financial reporting risks. This document was prepared in accordance with the guidance contained in the American Institute of Certified Public Accountants Statement on Standards for Attestation Engagements No. 16.

This description is intended to focus on the internal control structure of DMP that is relevant to their Print and Mail Production services customers only and does not encompass all aspects of the services provided or procedures followed by DMP.

Company Overview and Services Provided

Direct Mail Partners management has over 100 years of combined industry experience in print composition, policy and statement printing, electronic bill presentment and payment, mailing, presort, and direct mail. Working with clients in industries ranging from healthcare providers, health insurance companies, property and casualty insurance companies, financial services, utilities, manufacturers, retailers, distributors, municipalities, and associations means we have seen almost every situation before and have developed solutions to meet each and every need. With hundreds of active customers relying upon DMP for over 18 years, we have the experience and expertise to correctly produce your mission critical documents.

The control environment at DMP begins with management's philosophy and operating style as well as the priorities and direction provided by the executive management team. DMP's entire organization is dedicated to delivering the highest level of customer service. The company has created a corporate culture that supports this mission. DMP's stated objective for the control environment portion of the audit is that control activities provide reasonable assurance that discipline and structure are an integral part of the organization and influence the control consciousness of personnel.

Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people, who create, administer and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration and monitoring of other components. Integrity and ethical behavior are the products of the entity's ethical and behavioral standards, how they are communicated and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct and by leadership's example.

DMP has implemented, maintains and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest and expected standards of ethical and moral behavior. DMP's management conducts business dealings with employees, suppliers, customers, investors, creditors, competitors and auditors on a high ethical plane and insists others have similar business practices.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

DMP maintains job descriptions that contain requirements of knowledge and skills needed to adequately perform each job. DMP reinforces these requirements by providing a formal mentoring process that includes hands on training during the initial period of employment and continual hands on training for new business processes or job requirements.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristic. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions toward financial reporting (conservative or aggressive selection of alternative accounting principles and which accounting estimates are developed); and management's attitudes toward information processing and accounting functions and personnel. DMP's management takes a relatively conservative approach to information processing and risk associated with new business ventures.

Organizational Structure

An entity's organizational structure provides the framework for how entity wide objectives are planned, executed, controlled and monitored. A relevant organizational structure includes considering key areas of authority and responsibility and appropriate lines of reporting. An entity develops an organizational structure contingent, in part, on its size and nature of activities.

The responsibilities of key positions within DMP are clearly defined in documented job descriptions and communicated. Individuals that hold key positions are experienced, knowledgeable and have lengthy tenure with the company. DMP's organizational structure supports communication of information both up to leadership as well as down to support staff. DMP organizational structure is comprised of three primary business units and several groups that work together when delivering their Print and Mail Production services. The three business units consist of:

- Management Team are responsible for the oversight and monitoring of the organization's strategic direction and is responsible for making final decisions that are pushed down to the leadership team and ultimately to team members.
- Leadership Teams are responsible for the overall management, communications, direction and implementation of the management team's strategic direction. The leadership team is directly responsible for production and manages the quality of services.
- Team Members are responsible for executing on company tasks and managing the day to day service offerings of their respective departments.

Assignment of Authority and Responsibility

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements, including responsibility for information systems and authorizations for changes. Policies are established relating to business practices, knowledge and experience of key personnel and appropriate number of people to carry out duties. In addition, management's policies and communications are directed at ensuring that personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives and recognize how and for what they will be held accountable.

As mentioned above, DMP has well defined job descriptions and clear communication channels to disseminate information within the organization; this enables DMP to react to market and regulation changes and to meet its goals and objectives. DMP is appropriately staffed to support its operations, particularly with respect to critical areas such as software development and information technology system support.

Human Resource Policies and Practices

Human resource policies and practices relate to hiring, orientation, training, evaluating, counseling, promoting, compensating and remedial action. Also includes adequacy of employee back ground checks, particular with regard to prior actions or activities considered to be unacceptable by the entity.

Standards for hiring the most qualified individuals with emphasis on educational background, prior work experience, past accomplishments and evidence of integrity and ethical behavior demonstrate DMP's commitment to competent and trustworthy people. Training policies were created by DMP to communicate personnel roles and responsibilities and include practices such as regular training programs to illustrate expected level of performance, information technology appraisals and demonstrate DMP's commitment to advance qualified personnel to higher levels of responsibility. Personnel who work for DMP are required to read and acknowledge the company's internal policies and confidentiality requirements as well as the confidentiality of customer managed information.

Risk Assessment

Management is responsible for identifying the risks that threaten achievement of the control objectives stated in the management's description of the service organization's system. Management has implemented a process for identifying relevant risks. This process includes estimating the significance of identified risks, assessing the likelihood of their occurrence, and determining actions to address them. However, because control objectives relate to risk that controls seek to mitigate, management thoughtfully identified control objectives when designing, implementing, and documenting their system.

In order to identify the risk associated with each control objective, a risk level assessment is performed on the control activities found within the respective control objectives. For example, a control objective such as physical security is comprised of individual control activities. Each control activity is reviewed by management and departmental personnel to determine whether DMP's ability to adhere to the control activity as stated exists and the probability that DMP will maintain adherence using a scaling system of high, medium, and low. Management considers risks that can arise from both internal and external factors including:

Internal

- Potential human error
- Changes in the operating environment
- New personnel
- New or revamped information systems
- Rapid growth
- Funding of critical projects and ongoing operations
- Disruption of information systems processing and the extent to which backup systems are available and can be implemented
- New business models, products, or activities
- Corporate restructurings

External

- Changes of customer needs
- Natural disasters
- Carrier and utility outages
- Competition within market
- Payment Card Industry Data Security Standards
- National Automated Clearing House Association requirements
- Other privacy and processing rules and regulations

Information and Communication

Information Systems

A custom built architecture is in place to support DMP's print services. The DMP Production services are a complex environment with several pieces of large scale print and mail machinery, operating systems, databases and information systems. The Print and Mail Production services are managed by DMP at their headquarters in Dallas, Texas, however the infrastructure that is used to deploy the SFTP server and integration website services is located at a third party colocation data center managed by CoreXchange. The third party data center supports the physical and environmental controls and provides the network bandwidth and rack space used to deploy the file receipt function of the Print and Mail Production service.

DMP provides the software and administration of the system to ensure that the system processing operates as designed. Clients that utilize DMP Print and Mail Production services are responsible for data submissions, providing accurately formatted data files, and resolution of formatting issues.

DMP maintains their productions system through a continual evaluation of system development activities that includes a series of predefined software development procedures that includes initial request, requirement analysis, defined coding procedures, testing, deployment requirements and controlled access to production.

The Print and Mail Production services are deployed via the various business units within DMP. The day to day direct interactions with customers is delivered through DMP's Customer Service team who are responsible for the review of production jobs and providing support to DMP's clients. The Operations and Customer Service team members work directly with clients on the design and project requirements for their print and mail application ("template"); the Operations team is responsible for determining the

feasibility and managing the development of the application's requirements. The IT department is responsible for maintaining the networks, operating systems and databases for their internally managed and hosted computing environments.

DMP's above description of their information systems is supported by their control objectives and related controls described within the subsection below called "Control Objectives and Related Controls".

Communication

Throughout the organization, DMP conducts daily, weekly, monthly, quarterly and annual meetings to identify and address significant issues affecting the company's operations. Defined agendas, meeting minutes and a corporate information system are established vehicles used for addressing and monitoring activities, accomplishments and issues. As annual business development plans are established, annual meetings are held throughout the company to communicate defined goals and report results achieved. Monthly management meetings provide the vehicle for management to communicate and respond to operational tasks and issues. At all corporate levels, the company has established communication channels to promote and distribute information up and down the defined management structure.

Monitoring

An effective monitoring foundation is dependent on establishing an effective "tone at the top" of the organization and a high priority regarding effective internal controls. This requires that the top management team and the board of directors are involved in the evaluation process. Monitoring internal controls is dependent on the selection and utilization of evaluators which have a solid baseline understanding of internal controls. They also need to have suitable capabilities, resources and authority to conduct a meaningful assessment of internal controls.

DMP's monitoring of internal controls is performed through application of both ongoing evaluations and separate evaluations. These ongoing evaluations ascertain whether the components of their internal controls over services provided continue to function as designed and intended. In addition, these evaluations facilitate identification of internal control deficiencies and evaluators communicate findings to appropriate officials responsible for taking corrective action. DMP has continuous internal reporting, monitoring and evaluations procedures in place to identify deviations from internal controls to effectively report these deficiencies to appropriate departments.

Monitoring is a process of assessing risks linked to achieving operational objectives. This requires establishing a monitoring foundation consisting of procedures for evaluating risks to their user organizations. Monitoring activities include assessment of controls and reporting the results of the assessment together with any required corrective action steps.

DMP's monitoring procedures include:

- Periodic evaluation and testing of controls by their security department
- Continuous monitoring programs built into information systems.
- Analysis of and appropriate follow-up on, operating reports or metrics that might identify anomalies indicative of a control failure.
- Self-assessments by management regarding the tone they set in the organization and the effectiveness of their oversight functions.

- Quality assurance reviews of print operations, production issues, and internal security requirements.

Control Objectives and Related Controls

Physical Security

Control Objective 1: Control activities provide reasonable assurance that physical access to the business premises and information systems are limited to properly authorized individuals.

Physical security policy and procedures are documented and note physical access to business premises and on and off-site information systems is required to be restricted to authorized personnel based upon job responsibilities. To maintain compliance with the company policies, a badge access system is utilized at perimeter doors to restrict access to and within the corporate facility. Badge access is granted based upon management approval, required to be revoked upon termination, and reviewed quarterly to verify employees' access is appropriately restricted based upon their job duties.

Access to and throughout the business premises and processing areas is monitored through the use of security cameras and a third party alarm company as well as retention of visitor logs.

Computer Operations (System Availability)

Control Objective 2: Control activities provide reasonable assurance that production systems and equipment are designed, maintained and monitored to ensure system availability.

Operational, system build, outage, and recovery procedures are documented and made available to personnel to advise employees on the appropriate steps to take to ensure maximum system availability. Any issues are required to be documented within the help desk ticketing system, addressed, and resolved.

Appropriate environmental conditions and a periodic maintenance process for servers (upgrades/patches) and print equipment is required to be in place to reduce exposure to vulnerabilities and broken production equipment. Additionally, an Uninterruptible Power Supply ("UPS") battery backup is in place and regularly tested to allow for a controlled shutdown of production servers in event of power loss.

Antivirus software is installed on networked computers, regularly updated for the latest virus definitions and configured to perform regular scans.

Print Application Change Control

Control Objective 3: Control activities provide reasonable assurance that print applications ("templates") are developed to effectively support customer requirements and that changes are authorized and tested prior to production migration.

New print application implementation and modification policies and procedures are documented. The ticketing system is utilized to maintain and actively monitor progress of the Development, QA/Testing, Scheduling, Job Configuration/Setup, and Completion phases and approvals.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for configuration the accuracy of print application test / sample prior to promoting to production.
- User organizations are responsible for immediately notifying DMP of any inaccuracies or changes required to print applications.

Information Security

Control Objective 4: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

Formal information security policies and procedures are in place to establish organizational information security standards and logical access requirements. Administrative access to the network and key systems, servers, and applications is restricted to appropriate IT personnel. Access to the network, operating systems, databases, and applications must be approved by management and revoked upon termination.

Data Communications

Control Objective 5: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization

DMP makes use of stateful inspection firewalls at both the local server room and off-site data center, which are configured to prevent routable IP addresses on the internal network and limits traffic of services to and from specific destinations. Additionally, Virtual Private Network ("VPN"), SFTP, and site to site connections are required to be encrypted and limited appropriately. Changes to firewall rulesets and network devices require the review and approval of management. Additionally, external network scans are performed to identify any inappropriate configurations.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for providing accurate IP information during client on-boarding and notifying DMP of any IP changes.
- User organizations are required to maintain original copies of data provided to DMP.

Printing Process

Control Objective 6: Control activities provide reasonable assurance that printing orders received are processed and monitored throughout the production print and mailing process.

Print and mail operational procedures are documented and available to printing operations personnel. Files received through SFTP and other means are monitored and processed. IT and customer service personnel receive automated alerts if a processing error is identified. Issues are required to be logged and resolved.

The print production is managed using a work order system, which, one is created for each job processed detailing requirements and processing instructions. The work order is signed off by the employee who performed the work and supervisor at key phases to verify production quality and accuracy. Automated

validation checks and manual reconciliations are also performed to identify potential issues throughout the print production process.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for defining the communications method preferred to transmit data to DMP's systems (e.g., SFTP, Website).
- User organizations are responsible for transmitting data in the appropriate format.
- User organizations are responsible for notifying DMP of any issues (pulls, job stops, etc) noted after data transmission.

Production Print Systems and Data Access

Control Objective 7: Control activities provide reasonable assurance that logical access to print systems and data is restricted to authorized individuals.

Access to key functionality such as the creation of work orders, execution of print jobs, and the creation and modification of print applications is limited to appropriate personnel based upon job function. Additionally, access to client data on the SFTP server and throughout the network (including backup server) is limited to IT and other personnel on a need basis.

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for ensuring that user IDs and passwords for DMP systems are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.
- User organizations are responsible for notifying DMP of any user account modifications required.
- User organizations are responsible for providing the appropriate SFTP account information during setup.

Introduction

This report on the internal controls placed in operations and tests of operating effectiveness is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of DMP's controls that may be relevant to a user organization's internal control structure. This report, when combined with an understanding of the policies and procedures at user organizations, is intended to assist user auditors in planning the audit of the user organization and in assessing control risk for assertions of the user organizations' financial statement that may be affected by policies and procedures of DMP's Print and Mail Production services. The examination was performed in accordance with the AICPA SSAE No. 16, "*Reporting on Controls at a Service Organization".*

The system description, control objectives and related controls are the responsibility of DMP's management. Assurance Concepts' responsibility is to express an opinion that the system description was fairly presented and controls were suitably designed to achieve the control objectives specified in the Testing Matrices and were operating with sufficient effectiveness to provide reasonable, but not absolute, assurance that the control objectives, specified by DMP's management, were achieved during the period of July 1, 2012 to December 31, 2012.

Control Environment

The control environment represents the collective effect of various components in establishing and enhancing the effectiveness of specific controls and mitigating identified risks. In addition, to testing the design and operating effectiveness of the control activities in Section 4 of this report, our review also included tests of and consideration of the relevant components of DMP's control environment in support of their Print and Mail Production Services.

Our tests of the control environment included the following procedures to the extent we considered necessary to address management's relevant control environment and included the following:

- Obtaining an understanding of DMP's organizational structure, including the segregation of duties, policy statements and personnel policies.
- Discuss with management, operations, administrative and other personnel who were responsible for developing and enforces daily activities and requirements.
- Testing of oversight and company level controls on a sample basis to ensure key control environment activities were operating as described.

Testing Approach

The objective of our testing is to determine the operating effectiveness of the controls specified by DMP's management for the period of July 1, 2012 to December 31, 2012. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were achieved during the audit period. The nature of the tests conducted took into consideration the type of control testing and the evidential matter that is available to perform a test to determine the operating effectiveness.

Types of Tests Performed

1) **Inquiry:** tests include the corroboration of relevant personnel to verify the knowledge and understanding of the describe control activity.
2) **Observation:** tests include the physical observation of the implementation, application of or existence of specific controls.
3) **Inspection:** tests include the physical validation of documents, records, configuration or settings.
4) **Re-performance:** tests include the reprocessing of transactions, procedures and calculations to ensure the accuracy and completeness of the control description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by DMP:

Control Type and Frequency	Items to Test (Audit Period Six Months)	Item to Test (Audit Period > Six Months)
Manual control / many times per day	Minimum of 25	Minimum of 40
Manual control / daily	Minimum of 25	Minimum of 40
Manual control / weekly	Minimum of 5	Minimum of 10
Manual control / monthly	Minimum of 2	Minimum of 4
Manual control / quarterly	Minimum of 1	Minimum of 3
Manual control / annually	Per Occurrence	Per Occurrence
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
Application Controls	Test one operation of each application control if supported by effective IT general controls; otherwise test at lease 25	Test one operation of each application control if supported by effective IT general controls; otherwise test at lease 40

Testing Matrices

Physical Security

Control Objective 1: Control activities provide reasonable assurance that physical access to the business premises and information systems are limited to properly authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.1	Physical security policy and procedures are documented and note physical access to business premises and information systems is required to be restricted to authorized personnel based upon job responsibilities.	Inquired of CIO and COO and verified that they were documented and noted access to areas throughout the facility is authorized based upon job responsibility.	No relevant exceptions noted
		Inspected physical security policy and procedures and verified that they were documented and noted access to business premises and information systems was authorized based upon job responsibility.	No relevant exceptions noted
1.2	A badge access system is utilized at perimeter doors to restrict access to the corporate facility.	Observed access to the Corporate facility on a judgmentally selected sample of days and verified that a badge access system was utilized at perimeter doors and restricted access to the corporate facility.	No relevant exceptions noted
1.3	A review of badge access is performed quarterly to verify access to the business premises and information systems is appropriately restricted.	Inspected a judgmentally selected sample of quarterly badge access reviews and verified that physical access to the business premises and information systems was reviewed.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.4	A visitor access log is used to record the visitor name, company, purpose of visit, arrival and departure times.	Inquired of the CIO and COO and verified that visitors were required to record their name, company, purpose of visit, arrival and departure times upon entrance to the corporate facility.	No relevant exceptions noted
		Observed access to the Corporate facility on a judgmentally selected sample of dates and verified that visitors were required to complete the visitor access log upon entrance.	No relevant exceptions noted
1.5	Security cameras are in place to record activities to and within the facility. The security recordings are stored electronically for a minimum of seven days.	Inquired of the IT Systems Manager and verified that security cameras were in place and recorded activities to and within the facility. Security recordings were stored electronically and were available for a minimum of seven days.	No relevant exceptions noted
		Observed the Corporate facility and verified that security cameras were in place to record activities to and within the facility.	No relevant exceptions noted
		Observed the security camera system and verified recordings were stored electronically and were able to recall video from a minimum of 7 days prior.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.6	A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events.	Inquired of the CIO and COO and verified that a security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events.	No relevant exceptions noted
		Inspected the security alarm system contract and supporting invoices and verified a third party alarm monitoring provider was contracted throughout the period.	No relevant exceptions noted
1.7	New hires are provided access badges based upon job responsibilities. Access is approved by Management prior to issuance.	Inquired of COO and noted that badge access permissions were granted based upon job responsibilities and required to be approved by Management prior to issuance.	No relevant exceptions noted
		Inspected completed new hire form for a judgmentally selected sample of new hires during the audit period and verified that badge access permissions were granted based upon job responsibilities and approved by Management prior to issuance.	No relevant exceptions noted
1.8	Terminated employees' badge access rights are revoked as a component of the termination process.	Inquired of COO and noted that badge access rights revocation was a component of the termination process to prevent physical access to the facilities.	No relevant exceptions noted
		Inspected completed termination form and the active badge access listing for a judgmentally selected sample of terminated employees during the period and verified that badge access was revoked.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Production Area		
1.9	A badge access system is utilized at the production area's perimeter doors to restrict access to authorized personnel.	Observed access to the production area and verified that a badge access system was utilized at perimeter doors to restrict access to authorized personnel.	No relevant exceptions noted
1.10	Surveillance cameras are in place to record activity within the production area. Recordings are available for a minimum period of seven days.	Inquired of the IT Systems Manager and verified that security cameras were in place and recorded activities within the production area. Security recordings were stored electronically and were available for a minimum of seven days.	No relevant exceptions noted
		Observed the production area and verified that security cameras were in place to record activities.	No relevant exceptions noted
		Observed the security camera system and verified recordings of the production area cameras were stored electronically and were able to recall video from a minimum of 7 days prior.	No relevant exceptions noted
	Server Room		
1.11	A badge access system is utilized at the server room's perimeter doors to restrict access to authorized personnel.	Observed access to the server room and verified that a badge access system was utilized at the perimeter doors to restrict access to authorized personnel.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
1.12	Surveillance cameras record activity to and within the server room. Recordings are available for a minimum period of seven days.	Inquired of the IT Systems Manager and verified that security cameras were in place and recorded activities within the server room. Security recordings were stored electronically and were available for a minimum of seven days.	No relevant exceptions noted
		Observed the server room and verified that security cameras were in place to record activities.	No relevant exceptions noted
		Observed the security camera system and verified recordings of the server room cameras were stored electronically and were able to recall video from a minimum of 7 days prior.	No relevant exceptions noted

Computer Operations (System Availability)

Control Objective 2: Control activities provide reasonable assurance that production systems are designed, maintained and monitored to ensure system availability.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.1	Documented procedures are in place to guide operations personnel in performing daily activities to help ensure system availability.	Inquired of the IT Systems Manager and noted that documented procedures were in place to guide operations personnel in performing daily activities to help ensure system availability.	No relevant exceptions noted
		Inspected the DMP IT Policies and verified documented procedures were in place to guide operations personnel by establishment of a clear line of command and remediation steps to help ensure system availability.	No relevant exceptions noted
2.2	System build procedures are documented to guide personnel in the installation and maintenance of production servers.	Inquired of the IT Systems Manager and noted system requirements were documented to guide personnel in the installation and maintenance of production servers	No relevant exceptions noted
		Inspected the IT Disaster Recovery / Business Continuity procedures and verified system build procedures/requirements were documented to guide personnel in the installation and maintenance of production servers.	No relevant exceptions noted
2.3	System outage procedures are documented and in place to guide personnel in equipment outage resolution process.	Inquired of the IT Systems Manager and noted system outage/restoration procedures were documented in the failover, backup, and restoration procedure documents.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the IT Failover, Client & Production Backup, IT Disaster Recovery / Business Continuity, and Security Incident Response Plan documents and verified procedures were documented and in place to guide personnel through the equipment outage resolution process.	No relevant exceptions noted
2.4	A help desk ticketing system is utilized to track and respond to reported incidents.	Inquired of the IT Systems Manager and noted a help desk ticketing system was in place and utilized to track and respond to reported incidents.	No relevant exceptions noted
		Inspected signed statement and inquired of the Chief Information Officer and IT Systems Manager and noted that no significant security incidents occurred during the period.	No relevant exceptions noted
2.5	A patch management and release process is in place to monitor patch releases to production servers.	Inquired of the IT Systems Manager and noted the WSUS tool was used to maintain and monitor the patch management and release process to production servers.	No relevant exceptions noted
		Inspected the WSUS status report for a judgmentally selected sample of production servers and verified that a patch management and release process was in place to monitor patch releases to servers.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.6	The corporate facility is protected by fire detection and suppression systems that include: ➢ Fire alarm ➢ Water sprinklers ➢ Smoke detectors ➢ Hand-held fire extinguishers	Observed the corporate facility and verified that the following fire detection and suppression systems were in place: ➢ Fire alarm ➢ Water sprinklers ➢ Smoke detectors ➢ Hand-held fire extinguishers	No relevant exceptions noted
2.7	UPS provides power to production servers in the event of a temporary power outage or power surge.	Observed the server room and verified that the UPS was in place to provide power to production servers in event of a temporary power outage or power surge.	No relevant exceptions noted
2.8	The UPS is tested on a quarterly basis for functionality.	Inquired of the IT Systems Manager and verified that the UPS was tested quarterly to help ensure proper working order.	No relevant exceptions noted
		Inspected the quarterly UPS tests to verify that testing was performed to help ensure the device is in proper working order.	No relevant exceptions noted
	Antivirus		
2.9	Production servers are equipped with antivirus software to detect and prevent the transmission of data or files that contain certain virus signatures.	Inquired of the IT Systems Manager and verified that production servers were equipped with antivirus software.	No relevant exceptions noted
		Inspected the antivirus system's agent listing for a judgmentally selected sample of production servers and verified antivirus software was in place for the servers and workstations sampled.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
2.10	Antivirus software is configured to automatically update virus signatures to the latest version.	Inquired of the IT Systems Manager and verified that the antivirus software was configured to automatically update virus signatures with the latest version.	No relevant exceptions noted
		Observed the antivirus configuration and verified that the software was configured to automatically update virus signatures to the latest version.	No relevant exceptions noted
2.11	Antivirus software is configured to perform continuous and daily deep scans.	Inquired of the IT Systems Manager and verified that the antivirus software was configured to perform continuous and daily deep scans.	No relevant exceptions noted
		Observed the antivirus configuration and verified that active protection was enabled.	No relevant exceptions noted
		Observed the antivirus configuration and verified that deep scans were scheduled to be performed daily.	No relevant exceptions noted
		Inspected the antivirus system's recent scan listing for a judgmentally selected sample of production servers and verified antivirus software was actively scanning hosts.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Print and Mail Equipment Maintenance		
2.12	Print and Mail Equipment Manufacturers are contracted to perform maintenance and fixes on the production equipment.	Inquired of the COO and noted that Print and Mail Equipment Manufacturers were contracted to perform regular maintenance and fixes on the production equipment throughout the period.	No relevant exceptions noted
		Inspected the maintenance contracts for the production Print and Mail equipment and verified active agreements were in place to perform maintenance and fixes.	No relevant exceptions noted

Print Application Change Control

Control Objective 3: Control activities provide reasonable assurance that print applications ("templates") are developed to effectively support customer requirements and that changes are authorized and tested prior to production migration.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.1	Print job implementation and modification policies and procedures are documented.	Inquired of the COO and noted that print job implementation and modification policies and procedures were defined and documented.	No relevant exceptions noted
		Inspected the print job implementation and modification policies and procedures and verified that they were in place and noted the appropriate steps to take when configuring or modifying client print jobs.	No relevant exceptions noted
3.2	The ticketing system is utilized to maintain and track print job implementation / modification requests from customers.	Inquired of the COO and CIO and noted that a ticketing system was in place and utilized to maintain and track customer print job requests.	No relevant exceptions noted
		Inspected completed work order for a judgmentally selected sample of print job implementations / modification requests and verified that work orders were created in the ticketing system.	No relevant exceptions noted
	Change Request Initiation and Control		
3.3	A work order is created for each new print job implementation / modification to track tasks related to Development, QA/Testing, Scheduling, Job Configuration / Setup, and Completion.	Inquired of the COO and noted that a work order was required to be created for each print job implementation / modification to track completion of relevant tasks.	No relevant exceptions noted
		Inspected completed work order for a judgmentally selected sample of print job implementations / modifications and verified that work orders were created and used to track completion status.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Control of Changes		
3.4	Print job application development and testing efforts are performed in environments that are logically and/or virtually segregated from the production environment.	Inquired of the COO and IT Systems Manager and noted that development and testing efforts were performed in environments that were logically and/or virtually segregated from the production environment.	No relevant exceptions noted
		Inspected system generated listing of active servers on the network and verified print job application development and testing efforts were performed in an environment that were logically and/or virtually segregated from the production environment.	No relevant exceptions noted
	Testing		
3.5	Quality assurance testing is completed by Management, documented and approved prior to promoting to production.	Inquired of the COO and noted that samples were printed for new / modified jobs, reviewed, and approved prior to promoting to production.	No relevant exceptions noted
		Inspected completed work order for a judgmentally selected sample of print job implementations / modifications and verified that quality assurance testing was documented as completed and approved.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
3.6	User acceptance testing is completed by Client personnel, documented and approved prior to promoting to production.	Inquired of the COO and noted that user acceptance testing of new / modified jobs was completed by corresponding client and approved prior to promoting to production.	No relevant exceptions noted
		Inspected completed work order for a judgmentally selected sample of print job implementations / modifications and verified that user assurance testing was documented as completed and approved prior to promotion to production.	No relevant exceptions noted
	Final Approval		
3.7	Management approval is required prior to promoting to production.	Inquired of the COO and noted that Management was required to provide final approval prior to promoting any new / modified job to production.	No relevant exceptions noted
		Inspected completed work order for a judgmentally selected sample of print job implementations / modifications and verified that final approval was given by Management and documented prior to promoting to production.	No relevant exceptions noted

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for configuration the accuracy of print application test / sample prior to promoting to production.
- User organizations are responsible for immediately notifying DMP of any inaccuracies or changes required to print applications.

Information Security

Control Objective 4: Control activities provide reasonable assurance that logical access to critical systems and data is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
4.1	Formal information security policies and procedures are in place to establish organizational information security standards and logical access requirements.	Inspected the DMP information security and logical access policies and verified that organizational information security standards and logical access requirements were established.	No relevant exceptions noted
	Network Domain Authentication		
4.2	Network domain users are authenticated via an authorized user account and password. The network domain account policies are configured to enforce the following password requirements: ➢ Minimum password length of seven characters ➢ Minimum password history of 24 previously used passwords ➢ Maximum password age of 30 days ➢ Password complexity ➢ Lockout threshold of five consecutive failed login attempts	Inquired of the IT Systems Manager and verified that network domain users were required to authenticate using an authorized user account and password and that active directory controls access to network servers and applications.	No relevant exceptions noted
		Observed the Active Directory password configuration and verified that the following password requirements were defined: ➢ Minimum password length of seven characters ➢ Minimum password history of 24 previously used passwords ➢ Maximum password age of 30 days ➢ Password complexity ➢ Lockout threshold of five consecutive failed login attempts	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Network Domain Access		
4.3	Administrative access to the network domain is restricted to IT personnel based on their job responsibilities.	Inquired of IT Systems Manager and verified that administrative access to the network domain was restricted to IT personnel and granted based upon their job responsibilities.	No relevant exceptions noted
		Inspected system generated listing of network domain administrators and verified that access was restricted to appropriate IT personnel.	No relevant exceptions noted
4.4	Network accounts assigned to terminated personnel are deactivated upon notification of termination.	Inquired of the IT Systems Manager and verified that network accounts of terminated personnel were deactivated upon notification of termination.	No relevant exceptions noted
		Inspected a termination ticket for a judgmentally selected sample of terminated personnel and verified that network accounts were noted as deactivated or removed and signed off as completed.	No relevant exceptions noted
		Observed the Active Directory system and verified that the terminated employees sampled network access accounts were deactivated or removed.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Operating System Authentication		
4.5	Server operating system access is restricted via network domain credentials and group policy settings inherited from the primary domain controller.	Inquired of IT Systems Manager and noted that access to server operating systems was configured to restrict access via network domain credentials and that group policy settings were set to be inherited from the primary domain controller.	No relevant exceptions noted
		Inspected the group policy settings for the in scope production servers and verified that they were configured to inherit the group policy settings from the primary domain controller.	No relevant exceptions noted
		FTP Server Only: Inquired of IT Systems Manager and noted that the SFTP server was excluded from the network domain. Operating system level access to the SFTP server was secured using local user accounts and policy settings.	No relevant exceptions noted
		FTP Server Only: Inspected the firewall rules, group policy and password settings for the SFTP server and verified that the server was excluded from the network domain. Operating system level access to the SFTP server was secured using firewall rules and local user account permissions.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
	Operating System Access		
4.6	Administrative access to the server operating system is restricted to IT personnel based on their job responsibilities.	Inquired of IT Systems Manager and verified that administrative access to the in scope operating systems were restricted to IT personnel and granted based upon their job responsibilities.	No relevant exceptions noted
		Inspected system generated listing of network domain administrators verified that access was restricted to appropriate IT personnel.	No relevant exceptions noted
4.7	User access to server operating systems is revoked upon notification of termination.	Inquired of the IT Systems Manager and verified that network accounts of terminated personnel were deactivated upon notification of termination.	No relevant exceptions noted
		Inspected a termination ticket for a judgmentally selected sample of terminated personnel and verified that operating system level accounts were noted as deactivated or removed and signed off as completed.	No relevant exceptions noted
		Observed server operating system access and verified that the terminated employees' sampled operating system level accounts were deactivated or removed.	No relevant exceptions noted
4.8	Administrative access to the SFTP server where print files are stored is restricted to IT personnel based on their job responsibilities.	Inquired of IT Systems Manager and verified that administrative access to the SFTP server was restricted to IT personnel and granted based upon their job responsibilities.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed system generated listing of SFTP server administrators and verified that access was restricted to appropriate IT personnel.	No relevant exceptions noted
	Database Authentication		
4.9	Database users are authenticated via an authorized user account and password before being granted access. The databases are configured to enforce the following password requirements: ➢ Minimum password length of seven characters ➢ Minimum password history of 24 previously used passwords ➢ Maximum password age of 30 days ➢ Password complexity ➢ Lockout threshold of five consecutive failed login attempts	Inquired of the IT Systems Manager and verified that database users were required to authenticate using an authorized user account and password, based upon the group policy settings.	No relevant exceptions noted
		Observed the database password configuration and verified that the following password requirements were defined: ➢ Minimum password length of seven characters ➢ Minimum password history of 24 previously used passwords ➢ Maximum password age of 30 days ➢ Password complexity ➢ Lockout threshold of five consecutive failed login attempts	No relevant exceptions noted
	Database Access		
4.10	Administrative access to the databases is restricted to IT personnel based on their job responsibilities.	Inquired of IT Systems Manager and verified that administrative access to the databases was restricted to IT personnel and granted based upon their job responsibilities.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected system generated listing of database administrators from the production database servers and verified that access was restricted to appropriate IT personnel.	No relevant exceptions noted
4.11	Database access privileges are revoked as a component of the termination process.	Inquired of the IT Systems Manager and verified that network accounts of terminated personnel were deactivated upon notification of termination.	No relevant exceptions noted
		Inspected a termination ticket for a judgmentally selected sample of terminated personnel and verified that database access privileges were revoked upon notification of termination and noted as completed.	No relevant exceptions noted
		Observed database level access and verified that the terminated employees sampled database access privileges were deactivated or removed.	No relevant exceptions noted
	Application Authentication Controls		
4.12	Application authentication is inherited from the Active Directory.	Inquired of the IT Systems Manager and verified that application authentication was inherited from the Active Directory (Single Sign-On).	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Observed the active directory password configuration and verified that the following password requirements were defined: ➢ Minimum password length of seven characters ➢ Minimum password history of 24 previously used passwords ➢ Maximum password age of 30 days ➢ Password complexity ➢ Lockout threshold of five consecutive failed login attempts	No relevant exceptions noted
	Application Administration Access Controls		
4.13	Access to administer applications is limited to IT personnel based on their job responsibilities.	Inquired of IT Systems Manager and verified that administrative access to applications was limited to IT personnel and granted based upon their job responsibilities.	No relevant exceptions noted
		Inspected system generated listing of application level administrators and verified that access was restricted to appropriate IT personnel.	No relevant exceptions noted
	Access Provisioning		
4.14	Users are granted access to the network and systems based upon a completed access form approved by Management.	Inquired of IT Systems Manager and verified that access is only provisioned upon receipt of an appropriately approved access form.	No relevant exceptions noted
		Inspected completed access forms for a judgmentally selected sample of new hires and verified that access levels were approved by Management.	No relevant exceptions noted

Data Communications

Control Objective 5: Control activities provide reasonable assurance that data maintains its integrity and security as it is transmitted between third parties and the service organization.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.1	A stateful inspection firewall is in place and configured to filter unauthorized inbound network traffic from the Internet.	Inquired of the IT Systems Manager and verified that a stateful inspection firewall was in place and configured to filter unauthorized inbound network traffic from the internet.	No relevant exceptions noted
		Observed the firewall configurations and verified that the firewall was set to deny all traffic and required the use of predefined allow rules to appropriately filter traffic.	No relevant exceptions noted
5.2	NAT is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network.	Inquired of the IT Systems Manager and verified that a NAT policy was configured to manage internal IP addresses and prevent routable IP addresses from being allowed on the internal network.	No relevant exceptions noted
		Observed the firewall configurations and verified that NAT policies were utilized to manage internal IP addresses and prevent routable IP addresses from being allowed on the internal network.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.3	Administrative access to the firewall system is restricted to network administrators with firewall administration responsibilities.	Inquired of the IT Systems Manager and verified that administrative access to the firewalls was restricted to networking administrators with firewall administration responsibilities.	No relevant exceptions noted
		Inspected system generated listing of users with access to administer the firewall system and verified that access was appropriately restricted to network administrators with firewall administration responsibilities.	No relevant exceptions noted
5.4	Changes to firewall rulesets and network devices required the review and approval of management.	Inquired of the IT Systems Manager and verified that changes to firewall rulesets and network devices required the review and approval of management.	No relevant exceptions noted
		Inspected the firewall configuration change ticket for a judgmentally selected sample of firewall rule set and network device changes and verified changes were reviewed and approved.	No relevant exceptions noted
5.5	External network scans are performed on a quarterly basis.	Inquired of the IT Systems Manager and verified that external network scans were performed at least quarterly	No relevant exceptions noted
		Inspected the quarterly network scans and verified that scans were performed at least quarterly during the audit period.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.6	Customer SFTP sessions are encrypted using Advanced Encryption Standard AES-256.	Inquired of the IT Systems Manager and verified that the SFTP server was configured to encrypt customer SFTP sessions using AES-256.	No relevant exceptions noted
		Observed the SFTP configuration settings and verified that the SFTP server was configured to encrypt customer sessions using AES-256.	No relevant exceptions noted
5.7	Sessions between the SFTP server and DMP are encrypted using AES-256.	Inquired of the IT Systems Manager and verified that the site to site connection between the SFTP server and DMP office was configured to encrypt sessions using AES-256.	No relevant exceptions noted
		Observed the VPN Site to Site configuration settings and verified that connections between the SFTP server and DMP office were encrypted using AES-256.	No relevant exceptions noted
5.8	VPN sessions are encrypted using AES-256 w/ secure hash algorithm 1 ("SHA-1) authentication.	Inquired of the IT Systems Manager and verified that the VPN system was configured to encrypt sessions using AES-256 w/ SHA1 authentication.	No relevant exceptions noted
		Observed the VPN IPSEC configuration settings and verified that connections between the SFTP server and DMP office were encrypted using AES-256.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
5.9	Connections to the SFTP server are prevented for unknown IP addresses.	Inquired of the IT Systems Manager and verified that the SFTP server was configured to prevent connections from unknown IP addresses.	No relevant exceptions noted
		Inspected the Client SFTP Setup policy and verified that clients were required to undergo a formal authorization process that included obtaining and configuring their IP address within the SFTP server.	No relevant exceptions noted
		Observed the SFTP server IP rules configuration and verified that access to connect was restricted to only preconfigured IP addresses.	No relevant exceptions noted
		Observed attempt to access SFTP server from a non-permitted IP address and noted that the server rejected the connection.	No relevant exceptions noted

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for providing accurate IP information during client on-boarding and notifying DMP of any IP changes.
- User organizations are required to maintain original copies of data provided to DMP.

Printing Process

Control Objective 6: Control activities provide reasonable assurance that printing orders received are processed and handled from processing print files to printing final documents and shipping.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.1	Print and mail operational procedures are communicated to employees.	Inquired of COO and verified that print and mail operational procedures were communicated to operators as part of operator training, based upon function performed.	No relevant exceptions noted
		Inspected the print and mail training materials and verified that communicating operational procedures were communicated to employees.	No relevant exceptions noted
6.2	Automated notifications are sent to IT Support and Customer Service Representatives upon successful or failed file processing.	Inquired of COO and CIO and verified that automated notifications were configured to be sent to IT Support and Customer Service Representatives upon successful or failed file processing.	No relevant exceptions noted
		Observed the job processing configuration and sample success and failure alerts and verified that the system was configured to automatically send e-mail alerts to IT Support and Customer Service Representatives upon successful or failed file processing.	No relevant exceptions noted
6.3	Failed print file processing issues are logged and resolved.	Inquired of the CIO and verified that failed print file imports were monitored, logged by the operator, and resolved.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected evidence of resolution for a judgmentally selected sample of failed print file imports and verified that failed imports were resolved.	Exceptions noted – Unable to obtain a complete population of failed print file imports throughout the period. Selected a sample from the dates available and noted that failed print file processing issues were logged and resolved without exception.
6.4	A work order with customer information, job requirements, and processing instructions is utilized to document and monitor the progress of print orders.	Inquired of COO and verified that a work order with customer information, job requirements, and processing instructions was utilized to monitor the progress of print orders.	No relevant exceptions noted
		Inspected evidence of work order in place for a judgmentally selected sample of print jobs executed and verified that customer information, job requirements, and processing instructions were documented and utilized to document and monitor order progress.	No relevant exceptions noted
6.5	Print quality is reviewed and signed off by printing and mailroom operators prior to insertion.	Inquired of COO and verified that print quality is reviewed and signed off by printing and mailroom operators upon completion of print job.	No relevant exceptions noted
		Inspected the work order for a judgmentally selected sample of print jobs executed and verified that QC was performed for print quality and signed off as reviewed by print and/or mail room operators.	No relevant exceptions noted
6.6	The Account Manager performs a review of the work order form to verify completion of print job and quality assurance procedures prior to pre-sort and mailing.	Inquired of COO and noted that CSRs were required to sign off on work orders to verify completion of print job and quality assurance procedures prior to pre-sort and mailing.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the work order for a judgmentally selected sample of print jobs executed and verified that CSR review took place to note the completion of the job and that appropriate QA procedures took place prior to pre-sort and mailing.	No relevant exceptions noted
6.7	A Quick Response Code ("QR code") is appended to all pages in the job and read by the inserter to help ensure required documents are packaged appropriately.	Inquired of COO and noted that QR codes were appended to all pages in print jobs and used by the inserter machine to help ensure proper packaging of required documents.	No relevant exceptions noted
		Observed print job production on a judgmentally selected sample of days and verified printed pages contained a QR code that was read by the inserter when being processed to ensure appropriate packaging.	No relevant exceptions noted
6.8	Each impression is electronically counted at the end of the production printing process and reconciled to the work order to confirm that the job is balanced.	Inquired of COO and verified that print production operators were required to reconcile the expected and actual print counts and signed off to confirm job was balanced. Noted that deviations were expected to be noted and explained.	No relevant exceptions noted
		Inspected the work order for a judgmentally selected sample of print jobs executed and verified that reconciliations were performed of the expected count and actual counts to confirm jobs were balanced.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
6.9	A funds report is generated from the metering system and reconciled to the work order to confirm that the job is balanced.	Inquired of COO and noted that the metering machines produce a funds report upon completion of job and operators were required to reconcile to the count noted on the work order to confirm jobs were balanced.	No relevant exceptions noted
		Inspected the work order for a judgmentally selected sample of print jobs executed and verified that reconciliations were performed of the expected envelop count and actual stamps used and signed off to confirm that jobs were balanced.	No relevant exceptions noted
6.10	The pre-sort machine segregates mail with no postage affixed to help prevent return letters.	Inquired of COO and Operations Manager and noted that the presort machine is configured to reject letters without postage affixed to help prevent return letters.	No relevant exceptions noted
		Observed the pre-sort machine attempt to process mail without postage affixed and verified items were segregated into a separate basket.	No relevant exceptions noted

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for defining the communications method preferred to transmit data to DMP's systems (e.g., SFTP).
- User organizations are responsible for transmitting data in the appropriate format.
- User organizations are responsible for notifying DMP of any issues (pulls, job stops, etc) noted after data transmission.

Production Print Systems and Data Access

Control Objective 7: Control activities provide reasonable assurance that logical access to print systems and data is restricted to authorized individuals.

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.1	Print job files scheduled for production are restricted to personnel based on their job responsibilities.	Inquired of IT Systems Manager and noted that print job files scheduled for production were restricted to IT personnel and Management.	No relevant exceptions noted
		Observed the preprocessed folder and print files contained within and noted that files were stored in an encrypted format that were able to be read only by the print application, thus preventing inappropriate / unauthorized modification.	No relevant exceptions noted
		Observed access to folders where print job files scheduled for production were stored and verified access was restricted to IT and Management.	No relevant exceptions noted
7.2	Access to run print jobs is limited to production floor and IT personnel.	Inquired of IT Systems Manager and noted that access to execute print jobs was limited to production floor and IT personnel.	No relevant exceptions noted
		Observed access settings to the print job manager and verified access to execute print jobs was restricted to production floor and IT personnel.	No relevant exceptions noted
7.3	Access to client folders on the SFTP server is restricted to appropriate client, Customer Service and IT personnel.	Inquired of IT Systems Manager and noted that the SFTP server was configured to restrict access to customer data to appropriate client personnel.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
		Inspected the client SFTP Setup policy and verified that client SFTP accounts were configured to disallow access to all folders other than their corresponding folder.	No relevant exceptions noted
		Inspected access to a judgmentally selected sample of client folders on the SFTP server and verified access was restricted to appropriate client, customer service, and IT personnel.	No relevant exceptions noted
7.4	Access to modify and delete client data on the SFTP server is restricted to appropriate client personnel, Customer Service Representatives and IT.	Inquired of IT Systems Manager and noted that the SFTP server was configured to restrict access to modify and delete client data to appropriate client personnel.	No relevant exceptions noted
		Inspected access to a judgmentally selected sample of client folders on the SFTP server and verified access to modify and delete client data was restricted to appropriate client, customer service, and IT personnel.	No relevant exceptions noted
7.5	Access to setup and modify print job applications is restricted to appropriate IT personnel.	Inquired of IT Systems Manager and noted that access to setup and modify print job applications/configurations was restricted to appropriate IT personnel.	No relevant exceptions noted
		Observed access to the print processing systems and verified that access to setup and modify print job applications / configurations was restricted to appropriate IT personnel.	No relevant exceptions noted

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results
7.6	The ability to setup new print job applications / and promote application modifications in the production environment is restricted to a limited number of personnel without client service, sales, or print production responsibilities.	Inquired of IT Systems Manager and noted that access to setup new implementations / modifications in the production environment was restricted to a limited number of personnel without client service, sales, or print production responsibilities. Observed access to the print processing systems and verified that access to setup and modify print job applications / configurations was restricted to a limited number of personnel without client service, sales, or print production responsibilities.	No relevant exceptions noted No relevant exceptions noted

Complementary user entity controls. User entities are responsible for establishing controls related to the following:

- User organizations are responsible for ensuring that user IDs and passwords for DMP systems are assigned only to authorized individuals and that the roles assigned to the user account are appropriate.
- User organizations are responsible for notifying DMP of any user account modifications required.
- User organizations are responsible for providing the appropriate SFTP account information during setup.

Management's Response to Testing Exceptions

#	Control Activity Specified by the Service Organization	Test Applied by the Service Auditor	Test Results	Management's Response to Testing Exceptions
6.3	Failed print file processing issues are logged and resolved.	Inspected evidence of resolution for a judgmentally selected sample of failed print file imports and verified that failed imports were resolved.	Exceptions noted – Unable to obtain a complete population of failed print file imports throughout the period. Selected a sample from the dates available and noted that failed print file processing issues were logged and resolved without exception.	Management has put a process in place to automatically track failed print file imports through the help desk ticketing system to help ensure issues are appropriately logged.