# REPORT ON DMP BUSINESS PROCESS OUTSOURCING'S DESCRIPTION OF ITS PRINT AND MAIL PRODUCTION SYSTEM AND ON THE SUITABILITY OF THE DESIGN AND OPERATING EFFECTIVENESS OF ITS CONTROLS THROUGHOUT THE PERIOD APRIL 1, 2016 TO JUNE 30, 2017.

SKODA MINOTTI & CO.
CERTIFIED PUBLIC ACCOUNTANTS

Delivering on the Promise.

## DMP – SOC 1 Type II Table of Contents

# Acronym Table

| | |
|---|---|
| AES | Advanced Encryption Standard |
| AT-C | Attestation Standards. |
| DMP | DMP Business Process Outsourcing. |
| ID | Identification |
| IP | Internet Protocol |
| IT | Information Technology |
| NAT | Network Address Translation |
| QA | Quality Assurance |
| QC | Quality Control |
| QR | Quick Response |
| SFTP | Secure File Transfer Protocol |
| UPS | Uninterruptible Power Supply |
| VPN | Virtual Private Network |
| WSUS | Windows Server Update Services |

# Section 1: Independent Service Auditors’ Report

## Independent Service Auditors' Report

To: Management of DMP Business Process Outsourcing:

***Scope***

We have examined DMP Business Process Outsourcing's ("DMP" or the "service organization") description of its Print and Mail Production System entitled "DMP's Description of its Print and Mail Production System" for high integrity receipt, printing, and mailing of user entities' documents throughout the period April 1, 2016 to June 30, 2017, (description) and the suitability of the design and operating effectiveness of controls included in the description to achieve the related control objectives stated in the description, based on the criteria identified in "DMP's Assertion" (assertion). The controls and control objectives included in the description are those that management of DMP believes are likely to be relevant to user entities' internal control over financial reporting, and the description does not include those aspects of the Print and Mail Production that are not likely to be relevant to user entities' internal control over financial reporting.

DMP uses Zayo, a subservice organization, to provide colocation services for the Print and Mail Production. The description includes only the control objectives and related controls of DMP and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by DMP can be achieved only if complementary subservice organization controls assumed in the design of DMP's controls are suitably designed and operating effectively, along with the related controls at DMP. Our examination did not extend to controls of the subservice organization and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of DMP's controls are suitably designed and operating effectively, along with related controls at the service organization. Our examination did not extend to such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such complementary user entity controls.

***Service Organization's Responsibilities***

In section 2, DMP has provided an assertion about the fairness of the presentation of the description and suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description. DMP is responsible for preparing the description and its assertion, including the completeness, accuracy, and method of presentation of the description and 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 stated in the assertion, and designing, implementing, and documenting controls that are suitably designed and operating effectively to achieve the related control objectives stated in the description.

***Service Auditor's Responsibilities***

Our responsibility is to express an opinion on the fairness of the presentation of the description and on the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform the examination to obtain reasonable assurance about whether, in all material respects, based on the criteria in management's assertion, the description is fairly presented and the controls were suitably designed and operating effectively to achieve the related control objectives stated in the description throughout the period April 1, 2016 to June 30, 2017. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of a description of a service organization's system and the suitability of the design and operating effectiveness of controls involves

- performing procedures to obtain evidence about the fairness of the presentation of the description and the suitability of the design and operating effectiveness of the controls to achieve the related control objectives stated in the description, based on the criteria referenced above.
- assessing the risks that the description is not fairly presented and that the controls were not suitably designed or operating effectively to achieve the related control objectives stated in the description.
- testing the operating effectiveness of those controls that management considers necessary to provide reasonable assurance that the related control objectives stated in the description were achieved.
- evaluating the overall presentation of the description, suitability of the control objectives stated therein, and suitability of the criteria specified by the service organization in its assertion.

### *Inherent Limitations*

The description is prepared to meet the common needs of a broad range of user entities and their auditors who audit and report on user entities' financial statements and may not, therefore, include every aspect of the system that each individual user entity may consider important in its own particular environment. Because of their nature, controls at a service organization may not prevent, or detect and correct, all misstatements in processing or reporting transactions. Also, the projection to the future of any evaluation of the fairness of the presentation of the description, or conclusions about the suitability of the design or operating effectiveness of the controls to achieve the related control objectives, is subject to the risk that controls at a service organization may become ineffective.

### *Description of Tests of Controls*

The specific controls tested and the nature, timing, and results of those tests are listed in section 4.

### *Opinion*

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

*a.* the description fairly presents the Print and Mail Production System that was designed and implemented throughout the period April 1, 2016 to June 30, 2017.

*b.* the controls related to the control objectives stated in the description were suitably designed to provide reasonable assurance that the control objectives would be achieved if the controls operated effectively throughout the period April 1, 2016 to June 30, 2017, and the subservice organization and user entities applied the complementary controls assumed in the design of DMP's controls throughout the period April 1, 2016 to June 30, 2017.

c. the controls operated effectively to provide reasonable assurance that the control objectives stated in the description were achieved throughout the period April 1, 2016 to June 30, 2017, if complementary subservice organization and user entity controls assumed in the design of DMP's controls operated effectively throughout the period April 1, 2016 to June 30, 2017.

***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 DMP, user entities of DMP's Print and Mail Production System during some or all of the period April 1, 2016 to June 30, 2017, and their auditors who audit and report on such user entities' financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by user entities themselves, when assessing the risks of material misstatement of user entities' financial statements. This report is not intended to be and should not be used by anyone other than these specified parties.

/s/ SKODA MINOTTI & CO.
November 22, 2017
Tampa, Florida

# Section 2: DMP’s Assertion Statement for its Print and Mail Production System

## DMP’s Assertion

We have prepared the description of DMP’s Print and Mail Production System entitled "DMP Business Process Outsourcing’s Description of its Print and Mail Production System" for high integrity receipt, printing, and mailing of user entities' documents throughout the period April 1, 2016 to June 30, 2017, (description) for user entities of the system during some or all of the period April 1, 2016 to June 30, 2017, and their auditors who audit and report on such user entities’ financial statements or internal control over financial reporting and have a sufficient understanding to consider it, along with other information, including information about controls implemented by the subservice organization and user entities of the system themselves, when assessing the risks of material misstatement of user entities’ financial statements.

DMP Business Process Outsourcing uses Zayo, a subservice organization, to provide colocation services. The description includes only the control objectives and related controls of DMP and excludes the control objectives and related controls of the subservice organization. The description also indicates that certain control objectives specified by DMP can be achieved only if complementary subservice organization controls assumed in the design of DMP’s controls are suitably designed and operating effectively, along with the related controls at DMP. The description does not extend to controls of the subservice organization.

The description indicates that certain control objectives specified in the description can be achieved only if complementary user entity controls assumed in the design of DMP Business Process Outsourcing’s controls are suitably designed and operating effectively, along with related controls at the service organization. The description does not extend to controls of the user entities.

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

a. the description fairly presents the Print and Mail Production System made available to user entities of the system during some or all of the period April 1, 2016 to June 30, 2017, for processing their transactions as it relates to controls that are likely to be relevant to user entities’ internal control over financial reporting. 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 user entity transactions, including, if applicable,

(1) the types of services provided, including, as appropriate, the classes of transactions processed.

(2) the procedures, within both automated and manual systems, by which those services are provided, including, as appropriate, procedures by which transactions are initiated, authorized, recorded, processed, corrected as necessary, and transferred to the reports and other information prepared for user entities of the system.

(3) the information used in the performance of the procedures, including, if applicable, related accounting records, whether electronic or manual, and supporting information involved in initiating, authorizing, recording, processing, and reporting transactions; this includes the correction of incorrect information and how information is transferred to the reports and other information prepared for user entities.

(4) how the system captures and addresses significant events and conditions other than transactions.

(5) the process used to prepare reports and other information for user entities.

(6) services performed by a subservice organization, if any, including whether the inclusive method or the carve-out method has been used in relation to them.

(7) the specified control objectives and controls designed to achieve those objectives including, as applicable, complementary user entity controls assumed in the design of the service organization's controls.

(8) other aspects of our control environment, risk assessment process, information and communications (including the related business processes), control activities, and monitoring activities that are relevant to the services provided.

ii. includes relevant details of changes to the service organization's system during the period covered by the description.

iii. 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 user entities of the system and their user auditors and may not, therefore, include every aspect of the Print and Mail Production System that each individual user entity of the system and its auditor may consider important in its own particular environment.

b. the controls related to the control objectives stated in the description were suitably designed and operating effectively throughout the period April 1, 2016 to June 30, 2017, to achieve those control objectives if the subservice organization and user entities applied the complementary controls assumed in the design of DMP Business Process Outsourcing's controls throughout the period April 1, 2016 to June 30, 2017. 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 management of the service organization.

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

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

DMP Business Process Outsourcing, Inc.

/s/ Mark Depperschmidt

Chief Information Officer

November 22, 2017

# Section 3: DMP Business Process Outsourcing’s Description of its Print and Mail Production Service

## 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 Production System.

This report describes the system and control structure of DMP as it relates to their Print and Mail Production System. 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 clarified attestation standard AT-C Section 320.

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

## Company Overview and Services Provided

DMP Business Process Outsourcing 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.

## System Description

## Subservice Organization

The following subservice organization is utilized to assist in the delivery of DMP's Print and Mail Production System from April 1, 2016 to June 30, 2017:

- Zayo – Colocation Data Center

DMP uses Zayo Colocation Data Center. The subservice organization is responsible for providing reasonable assurance that power, cooling, and network availability, and physical security is provided to the collocated systems.

The applicable controls relating to the control objectives that are intended to be met by the subservice organization, alone or in combination with controls at DMP, and the types of control expected to be implemented at the subservice organizations to meet those controls are described in the table below. On an annual basis, DMP reviews Zayo's SOC Report and visits the data center site. If there are exceptions or controls not operating effectively at a subservice organization this risk is incorporated into a risk assessment and appropriate actions are taken to mitigate risks in the future.

| Control Activities and Related Control Objectives Expected to be Implemented by Zayo | Applicable Control Objective |
|---|---|
| Subservice organizations are responsible for providing reasonable assurance that production systems and equipment hosting the collocated servers are designed, maintained and monitored to ensure system availability. | Computer Operations (System Availability) |
| The subservice organization is responsible for restricting physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers. | Physical Security |
| The subservice organization is responsible for environmental controls used to support the availability of the data center power and intranet services. | Environmental Security |

### Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an organization and the way personnel conduct their activities, influencing how they carry out their control functions.  This is the foundation for all other components of internal control, providing discipline and structure for the business operations.

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 System. 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 Production 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 System 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 Zayo. 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 System are responsible for data submissions, providing accurately formatted data files, and resolution of formatting issues.

DMP maintains their production 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 System 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 its information systems is supported by its 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 members 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 its 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.

### 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.

### 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.

### 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.

## User Entity Control Considerations

DMP’s Print and Mail Production System control framework was designed with the assumption that specific internal controls would be implemented by client organizations. In certain situations, the application of specified internal controls at client organizations is necessary to achieve the specific control objectives included in this report. The client's organizational internal controls should be operational to complement DMP's Print and Mail Production System controls. Skoda Minotti's examination was limited to the activities and procedures for DMP's Print and Mail Production System as they relate to their clients. Accordingly, Skoda Minotti's examination did not extend to any activities or procedures in place at the clients of DMP. It is each interested party's responsibility to evaluate the client organization control considerations information presented in this section in relation to the internal controls that are in place at client organizations to obtain a complete understanding of the total internal control structure and to assess control risk. If effective client internal controls are not in place, DMP's Print and Mail Production System controls may not compensate for such weaknesses.

This section describes other internal controls that should be in operation at client organizations to complement the controls at DMP's Print and Mail Production System. The auditors of DMP's Print and Mail Production System clients should consider whether the following controls have been placed in operation at client organizations.

*Print Application Change Control*

- 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.

*Data Communications*

- 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

- 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 System Data Access*

- 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.

# Section 4: DMP’s Control Objectives and Related Controls and Independent Service Auditors’ Tests of Controls and Results Thereof

## 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 System. The examination was performed in accordance with the American Institute of Certified Public Accountants clarified attestation standard AT-C Section 320, "Reporting on an Examination of Controls at a Service Organization Relevant to User Entities' Internal Control over Financial Reporting."

The system description, control objectives and related controls are the responsibility of DMP's management. Skoda Minotti's 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 April 1, 2016 to June 30, 2017.

## 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 System.

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 April 1, 2016 to June 30, 2017. 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 (Examination Period 12 Months) |
|---|---|
| Occurrence based | 10%, minimum of 5, maximum of 25 |
| Manual control performed weekly | 5 |
| Manual control performed monthly | 2 |
| Manual control performed quarterly | 2 |
| Manual control performed annually | 1 |
| Application/Programmed control | Test one application of each programmed control for each type of transaction if supported by effective IT general controls (that have been tested); otherwise test at least 25 |

# 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. | Inspected physical security policy and procedures to verify that they were documented to verify access to business premises and information systems was authorized based upon job responsibility. | No 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 to verify that a badge access system was utilized at perimeter doors and restricted access to the corporate facility. | No 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 quarterly badge access reviews for a sample of quarters throughout the examination period to verify that physical access to the business premises and information systems was reviewed. | No exceptions noted. |
| 1.4 | A visitor access log is used to record the visitor name, company, purpose of visit, arrival and departure times. | Inspected visitor access logs to verify that visitors were required to record their name, company, purpose of visit, arrival and departure times upon entrance to the corporate facility. | No 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. | Inspected the camera monitoring module to verify that security cameras were in place and recorded activities to and within the facility. Security recordings were stored electronically and were able to recall video from a minimum of seven days prior. | No exceptions noted. |
| 1.6 | A security alarm system is installed and monitored by a third party alarm monitoring provider to detect unauthorized events. | Inspected the security alarm system contract and supporting invoices to verify a third party alarm monitoring provider was contracted throughout the period. | No exceptions noted. |
| 1.7 | New hires are provided access badges based upon job responsibilities. Access is approved by Management prior to issuance. | Inspected completed new hire form for a sample of employees hired throughout the examination period to verify that badge access permissions were granted to the selected employees based upon job responsibilities and Management approval. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| 1.8 | Terminated employees’ badge access rights are revoked as a component of the termination process. | Inspected completed termination form and the active badge access listing for a sample of employees terminated throughout the examination period to verify that badge access was revoked. | No exceptions noted. |
| | **<u>Production Area</u>** | | |
| 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 to verify that a badge access system was utilized at perimeter doors to restrict access to authorized personnel. | No 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. | Observed the production area to verify that security cameras were in place to record activities. | No exceptions noted. |
| | | Inspected the camera monitoring module to verify that security cameras were in place and recorded activities within the production area. Security recordings were stored electronically and were able to recall video from a minimum of seven days prior. | No exceptions noted |
| | **<u>Server Room</u>** | | |
| 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 exceptions noted. |
| 1.12 | Surveillance cameras record activity to and within the server room.  Recordings are available for a minimum period of seven days. | Observed the server room and verified that security cameras were in place to record activities. | No 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 seven days prior. | No 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. | Inspected the IT Policies to verify 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 exceptions noted. |
| 2.2 | System build procedures are documented to guide personnel in the installation and maintenance of production servers. | Inspected the IT Disaster Recovery/Business Continuity procedures to verify system build procedures/requirements were documented to guide personnel in the installation and maintenance of production servers. | No exceptions noted. |
| 2.3 | System outage procedures are documented and in place to guide personnel in equipment outage resolution process. | Inspected the IT Failover, Client & Production Backup, IT Disaster Recovery/Business Continuity, and Security Incident Response Plan documents to verify procedures were documented and in place to guide personnel through the equipment outage resolution process. | No exceptions noted. |
| 2.4 | A help desk ticketing system is utilized to track and respond to reported incidents. | Inspected a sample of help desk tickets to resolve production issues throughout the examination period to verify a system was in place to track and respond to reported incidents. | No exceptions noted. |
| 2.5 | A patch management and release process is in place to monitor patch releases to production servers. | Inspected the WSUS status report for a sample of production server’s active throughout the examination period to verify that a patch management and release process was in place to monitor patch releases to servers. | No 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:<br>➢ Fire alarm<br>➢ Water sprinklers<br>➢ Smoke detectors<br>➢ Hand-held fire extinguishers | Observed the corporate facility and verified that the following fire detection and suppression systems were in place:<br>➢ Fire alarm<br>➢ Water sprinklers<br>➢ Smoke detectors<br>➢ Hand-held fire extinguishers | No 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 to verify that an UPS was in place to provide power to production servers in event of a temporary power outage or power surge. | No exceptions noted. |
| 2.8 | The UPS is tested on a quarterly basis for functionality. | Inspected the UPS tests for a sample of quarters throughout the examination period to verify that testing was performed to help ensure the device is in proper working order for the selected quarter. | No 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. | Inspected the antivirus system's agent listing for a sample of production servers to verify antivirus software is in place at the organization to detect and prevent the transmission of data or files that contain certain virus signatures. | No exceptions noted. |
| 2.10 | Antivirus software is configured to automatically update virus signatures to the latest version. | Inspected the antivirus configuration to verify that the software was configured to automatically update servers to the latest version.<br>Observed the antivirus configuration and verified that the software was configured to automatically update virus signatures to the latest version. | No exceptions noted. |
| 2.11 | Antivirus software is configured to perform continuous and daily deep scans. | Inspected the antivirus system's recent scan listing for a sample of production servers to verify antivirus software was actively scanning hosts.<br>Observed the antivirus configuration and verified that deep scans were scheduled to be performed daily. | No 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. | Inspected the maintenance contracts for the production print and mail equipment to verify active agreements were in place to perform maintenance and fixes. | No 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. | Inspected the print job implementation and modification policies and procedures to verify that they were in place to verify the appropriate steps to take when configuring or modifying client print jobs. | No exceptions noted. |
| 3.2 | The ticketing system is utilized to maintain and track print job implementation/modification requests from customers. | Inspected completed work order for a sample of print job implementations/modification requests tickets throughout the examination period to verify that work orders were created, tracked, and resolved in the ticketing system. | No 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. | Inspected completed work order for a selected sample of print job implementations/modifications throughout the examination period to verify that work orders were created and used to track completion status for the selected samples. | No exceptions noted. |
| | **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. | Inspected system generated list 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 exceptions noted. |
| | **Testing** | | |
| 3.5 | Quality assurance testing is completed by Management, documented and approved prior to promoting to production. | Inspected completed work order for a selected sample of print job implementations/modifications to verify that quality assurance testing was documented as completed and approved. | No 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. | Inspected completed work order for a selected sample of print job implementations/modifications to verify that user assurance testing was documented as completed and approved. | No exceptions noted. |
|  | **Final Approval** |  |  |
| 3.7 | Management approval is required prior to promoting to production. | Inspected completed work order for a selected sample of print job implementations/modifications to verify that final approval was given by Management and documented prior to promoting to production. | No 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 to verify that organizational information security standards and logical access requirements were established. | No 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:<br>➢ Minimum password length of eight characters<br>➢ Minimum password history of 12 previously used passwords<br>➢ Maximum password age of 90 days<br>➢ Password complexity<br>➢ Lockout threshold of five consecutive failed login attempts | Inspected the Active Directory password configuration and verified that the following password requirements were defined:<br>➢ Minimum password length of eight characters<br>➢ Minimum password history of 12 previously used passwords<br>➢ Maximum password age of 90 days<br>➢ Password complexity<br>➢ Lockout threshold of five consecutive failed login attempts | No 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. | Inspected system generated listing of network domain administrators and verified that access was restricted to appropriate IT personnel. | No exceptions noted. |
| 4.4 | Network accounts assigned to terminated personnel are deactivated upon notification of termination. | Inspected user access report and supporting termination ticket for a sample of personnel terminated throughout the examination period to verify that termination forms were completed to notify IT personnel of termination. | No exceptions noted. |
| | **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. | 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.<br>Inspected the firewall rules, group policy, and password settings for the SFTP server to verify 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 exceptions noted. |
| | **Operating System Access** | | |
| 4.6 | Administrative access to the server operating system is restricted to IT personnel based on their job responsibilities. | Inspected system generated list of network domain administrators to verify that access was restricted to appropriate IT personnel. | No exceptions noted. |
| 4.7 | User access to server operating systems is revoked upon notification of termination. | Inspected server operating system access and supporting termination ticket for a sample of employees terminated throughout the examination period to verify that operating system level accounts were noted as deactivated or removed and signed off as completed. | No 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. | Inspected system generated list of SFTP server administrators to verify that access was restricted to appropriate IT personnel.<br>Inspected system generated listing of SFTP server administrators to verify that access was restricted to appropriate | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
|  |  | IT personnel. |  |
|  | **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:<br>➢ Minimum password length of seven characters<br>➢ Minimum password history of 12 previously used passwords<br>➢ Maximum password age of 90 days<br>➢ Password complexity<br>➢ Lockout threshold of five consecutive failed login attempts | Inspected the database password configuration and verified that the following password requirements were defined:<br>➢ Minimum password length of seven characters<br>➢ Minimum password history of 12 previously used passwords<br>➢ Maximum password age of 90 days<br>➢ Password complexity<br>➢ Lockout threshold of five consecutive failed login attempts | No exceptions noted. |
|  | **Database Access** |  |  |
| 4.10 | Administrative access to the databases is restricted to IT personnel based on their job responsibilities. | Inspected system generated list of database administrators from the production database servers to verify that access was restricted to appropriate IT personnel. | No exceptions noted. |
| 4.11 | Database access privileges are revoked as a component of the termination process. | Inspected database access and supporting termination ticket for a sample of employees terminated throughout the examination period to verify that database access privileges were revoked upon notification of termination to verify as completed. | No exceptions noted. |
|  | **Application Authentication Controls** |  |  |
| 4.12 | Application authentication is inherited from the Active Directory. | Inspected the Active Directory password configuration applied to the production applications to verify user authentication was inherited from Active Directory. | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | **Application Administration Access Controls** | | |
| 4.13 | Access to administer applications is limited to IT personnel based on their job responsibilities. | Inspected system generated list of application level administrators to verify that access was restricted to appropriate IT personnel. | No exceptions noted. |
| | **Access Provisioning** | | |
| 4.14 | Users are granted access to the network and systems based upon a completed access form approved by Management. | Inspected completed access forms for a sample personnel hired throughout the examination period to verify that access levels were approved by Management. | No exceptions noted. |
| 4.15 | The applications are configured to log certain user account application activities and logs are available for ad hoc review purposes. | Inspected user account activities for applications in place to support the system to verify that applications are configured to record user activity and the logs are available for ad hoc review. | No 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. | Inspected 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 exceptions noted. |
| 5.2 | NAT is utilized to manage internal IP addresses and routable IP addresses are not permitted on the internal network. | Inspected 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 exceptions noted. |
| 5.3 | Administrative access to the firewall system is restricted to network administrators with firewall administration responsibilities. | Inspected system generated list of users with access to administer the firewall system to verify that access was appropriately restricted to network administrators with firewall administration responsibilities. | No exceptions noted. |
| 5.4 | Changes to firewall rulesets and network devices required the review and approval of management. | Inspected the firewall configuration change ticket for a sample of firewall rule set and network device changes to verify changes are reviewed and approved. | No exceptions noted. |
| 5.5 | External network scans are performed on a quarterly basis. | Inspected a selected sample of quarterly network scans to verify that scans were performed quarterly. | No exceptions noted. |
| 5.6 | Customer SFTP sessions are encrypted using Advanced Encryption Standard AES-256. | Observed the SFTP configuration settings to verify that the SFTP server was configured to encrypt customer sessions using AES-256. | No exceptions noted. |
| 5.7 | Sessions between the SFTP server and DMP are encrypted using AES-256. | Observed the VPN Site to Site configuration settings to verify that connections between the SFTP server and DMP office were | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | encrypted using AES-256. | |
| 5.8 | VPN sessions are encrypted using AES-256 with secure hash algorithm 1 (“SHA-1”) authentication. | Observed the VPN IPSEC configuration settings to verify that connections between the SFTP server and DMP office were encrypted using AES-256 and SHA-1. | No exceptions noted. |
| 5.9 | Connections to the SFTP server are prevented for unknown IP addresses. | 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.<br>Inspected the SFTP server IP rules configuration and verified that access to connect was restricted to only preconfigured IP addresses. | No 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 throughout 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. | Inspected the print and mail training materials and verified that communicating operational procedures were communicated to employees. | No exceptions noted. |
| 6.2 | Automated notifications are sent to IT Support and Customer Service Representatives upon successful or failed file processing. | Inspected the job processing configuration and sample success and failure alert to verify that the system was configured to automatically send an e-mail alert to IT and/or Customer Support personnel upon successful or failed file processing. | No exceptions noted. |
| 6.3 | Failed print file processing issues are logged and resolved. | Inspected evidence of resolution for a sample of failed print file imports and verified that failed imports were resolved. | No exceptions noted. |
| 6.4 | A work order with customer information, job requirements, and processing instructions is utilized to document and monitor the progress of print orders. | Inspected evidence of work order in place for a selected sample of  print jobs executed to verify that customer information, job requirements, and processing instructions were documented and utilized to document and monitor order progress. | No exceptions noted. |
| 6.5 | Print quality is reviewed and signed off by printing and mailroom operators prior to insertion. | Inspected the work order for a sample of  print jobs executed throughout the examination period to verify that QC was performed for print quality and signed off as reviewed by print and/or mail room operators. | No 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. | Inspected the work order for a selected sample of print jobs executed to verify 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 exceptions noted. |
| 6.7 | A QR code is appended to all pages in the job to help ensure required documents are packaged appropriately. | Observed print job production to verify printed pages contained a QR code that was read by the inserter when being processed to | No exceptions noted. |

| # | Control Activity Specified by the Service Organization | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|
| | | ensure appropriate packaging. | |
| 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. | Inspected the work order for a sample of print jobs executed throughout the examination period to verify that reconciliations were performed of the expected count and actual count to confirm jobs were balanced. | No exceptions noted. |
| 6.9 | A funds report is generated from the metering system and reconciled to the work order to confirm that the job is balanced. | Inspected the work order for a selected sample of  print jobs executed throughout the examination period to verify that reconciliations were performed of the expected envelop count and actual stamps used and signed off to confirm that jobs were balanced. | No 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. | 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 exceptions noted. |
| 7.2 | Access to run print jobs is limited to production floor and IT personnel. | Observed access settings to the print job manager and verified access to execute print jobs was restricted to production floor and IT personnel. | No exceptions noted. |
| 7.3 | Access to client folders on the SFTP server is restricted to appropriate client, Customer Service and IT personnel. | Inspected the client SFTP Setup policy to verify that client SFTP accounts were configured to disallow access to all folders other than their corresponding folder.<br>Inspected access to a sample of client folders on the SFTP server to verify access was restricted to appropriate client, customer service, and IT personnel. | No 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. | Inspected access to a 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 exceptions noted. |
| 7.5 | Access to setup and modify print job applications is restricted to appropriate IT personnel. | Inspected 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 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. | Inspected access to the print processing systems to verify 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 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.