Thoropass™
Assurance

DIS Direct
Data-Driven Direct Mail Solutions

System and Organization Controls

(SOC) 2 Type 2 Report

Digital Imaging Solutions Inc.'s Description of the DIS Direct Service and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period February 1, 2025 to January 31, 2026

TABLE OF CONTENTS

SECTION 1

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Digital Imaging Solutions Inc. ("DIS Direct" or "the Company")

Scope

We have examined DIS Direct's accompanying description of the DIS Direct Service found in Section 3 titled "Description of the DIS Direct Service Throughout the Period February 1, 2025 to January 31, 2026" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria (description criteria)* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that DIS Direct's service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

DIS Direct uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DIS Direct, to achieve DIS Direct's service commitments and system requirements based on the applicable trust services criteria. The description presents DIS Direct's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DIS Direct's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

DIS Direct is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that DIS Direct's service commitments and system requirements were achieved. In Section 2, DIS Direct has provided the accompanying assertion titled "Assertion of Digital Imaging Solutions Inc. Management" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. DIS Direct is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls 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 our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were

achieved based on the applicable trust services criteria. 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 the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- Evaluating the overall presentation of the description.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We are required to be independent and to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement, including the Code of Professional Conduct established by the AICPA, and we have complied with those requirements. In addition, we applied the Statements on Quality Control Standards established by the AICPA, and, accordingly, maintain a comprehensive system of quality control.

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are listed in Section 4, "Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security Category" of this report.

Controls That Were Not Tested During the Period

The Company's description of its system discusses the following controls implemented and operated during the period February 1, 2025 to January 31, 2026 that were not tested as part of our procedures:

- REQ-8: Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.
- REQ-10: Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement
- REQ-11: New employees offered employment are subject to background checks prior to their start date.
- REQ-12: New employees complete security awareness training upon hire.
- REQ-30: Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.
- REQ-31: Access to system components is revoked within 24 hours of termination as part of the termination process.
- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.

During the period February 1, 2025 to January 31, 2026, the Company did not experience the above control activities that would warrant the operation of the controls during the period.

Because the controls described above were not required to operate during the period, we did not test the operating effectiveness of those controls as evaluated using the following trust services criteria (TSC):

- TSC CC1.1: The entity demonstrates a commitment to integrity and ethical values.
- TSC CC1.4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
- TSC CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
- TSC CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.

Opinion

In our opinion, in all material respects—

a. The description presents the DIS Direct Service that was designed and implemented throughout the period February 1, 2025 to January 31, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that DIS Direct's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of DIS Direct's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that DIS Direct's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of DIS Direct's controls operated effectively throughout that period.

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 DIS Direct, user entities of the DIS Direct Service during some or all of the period February 1, 2025 to January 31, 2026, business partners of DIS Direct subject to risks arising from interactions with the DIS Direct Service, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization.
- How the service organization's system interacts with user entities, business partners, subservice organizations, and other parties.
- Internal control and its limitations.
- Complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
- The applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

Thoropass Assurance

Arlington, Virginia
February 2, 2026

SECTION 2

Assertion of Digital Imaging Solutions Inc. Management

Assertion of Digital Imaging Solutions Inc. Management

We have prepared the accompanying description in Section 3 titled "Description of the DIS Direct Service Throughout the Period February 1, 2025 to January 31, 2026" (description), based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria (description criteria)*. The description is intended to provide report users with information about the DIS Direct Service that may be useful when assessing the risks arising from interactions with DIS Direct's system, particularly information about system controls that DIS Direct has designed, implemented and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria*.

DIS Direct uses a subservice organization for infrastructure and data hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at DIS Direct, to achieve DIS Direct's service commitments and system requirements based on the applicable trust services criteria. The description presents DIS Direct's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of DIS Direct's controls. The description does not disclose the actual controls at the subservice organization.

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

a. The description presents the DIS Direct Service that was designed and implemented throughout the period February 1, 2025 to January 31, 2026, in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that DIS Direct's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization applied the complementary controls assumed in the design of DIS Direct's controls throughout that period.
c. The controls stated in the description operated effectively throughout the period February 1, 2025 to January 31, 2026, to provide reasonable assurance that DIS Direct's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls assumed in the design of DIS Direct's controls operated effectively throughout that period.

Our description of the DIS Direct Service discusses the following controls implemented during the period February 1, 2025 to January 31, 2026 that were not required to operate due to non occurrence of the activities:

- REQ-8: Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.
- REQ-10: Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement
- REQ-11: New employees offered employment are subject to background checks prior to their start date.
- REQ-12: New employees complete security awareness training upon hire.
- REQ-30: Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.
- REQ-31: Access to system components is revoked within 24 hours of termination as part of the termination process.
- REQ-50: All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.

During the period February 1, 2025 to January 31, 2026, DIS Direct did not experience the above control activities that

would warrant the operation of the controls during the period.

Digital Imaging Solutions Inc.

SECTION 3

Description of the DIS Direct Service

Description of the DIS Direct Service Throughout the Period February 1, 2025 to January 31, 2026

Overview of Operations

Digital Imaging Solutions Inc. ("DIS Direct" or "the Company") is a business-to-business and business-to-consumer commercial printing and direct mail services provider that serves marketers, advertisers, and organizations with high-volume mailing needs. DIS Direct operates as a full-service direct mail partner, offering end-to-end printing, data processing, and mailing fulfillment services that support clients' targeted campaigns and communications.

At its core, the DIS Direct Service consists of high-volume printing and direct mail production, leveraging advanced printing technology such as web offset presses with inline variable data capabilities to produce custom print pieces at scale with high precision and color quality. The service supports a broad range of direct mail formats, including postcards, self-mailers, brochures, flyers, envelopes, and specialty items such as door hangers and snap pack mailers — all tailored to meet specific campaign objectives and audience requirements.

DIS Direct also offers integrated lettershop and mailing services that bring together all elements of a direct mail campaign. This includes insertion, assembly, personalization, address data processing and list maintenance, postal optimization, and pre-sorting to ensure efficient entry into the mailstream and competitive postage rates. The Company's expertise in postal logistics and audience data processing helps customers streamline operations from print production through delivery.

The DIS Direct Service supports variable data printing and data-driven campaign execution, enabling organizations to tailor content and offers at the individual recipient level based on audience lists and targeting criteria. The service can also integrate with digital engagement features such as USPS Informed Delivery, which enables recipients to preview mail pieces digitally before they arrive, adding a complementary digital dimension to traditional direct mail.

DIS Direct is headquartered in Itasca, Illinois, and its solutions are positioned to serve a wide range of industries, including retail, political advocacy, non-profit organizations, and corporate marketing functions that require precision and scale in printed communications.

The system description in this section of the report details the DIS Direct Service. Any other Company services are not within the scope of this report. The accompanying description includes only the policies, procedures, and control activities at the Company and does not include the policies, procedures, and control activities at any subservice organizations (see below for further discussion of the subservice organization).

Principal Service Commitments and System Requirements

Service commitments are declarations made by management to customers regarding the performance and security of the DIS Direct Service. The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers.

System requirements are specifications that define how the DIS Direct Service is designed and operated in order to meet the Company's principal commitments to customers. These requirements are specified in the Company's policies and procedures, system design documentation, contractual obligations, and applicable laws and regulations.

The Company's principal service commitments and system requirements related to the DIS Direct Service include the following:

Security Service Commitment and System Requirements

DIS Direct will take responsibility for implementing appropriate technical and organizational safeguards to ensure the protection of sensitive information.

To meet this commitment, the Company has established system requirements, including:

- Change Management
- Encryption Standards
- Identity and Access Management
- Network Security and Segmentation
- Policy Management and Governance
- Security Awareness Training
- Security Incident Response
- Security Monitoring and Reporting
- Threat and Vulnerability Management
- Vendor Risk Management

The Components of the System Used to Provide the Service

The boundaries of the DIS Direct Service include the aspects of the Company's infrastructure, software, people, procedures, and data that are necessary to deliver the service and directly support its operation. Supporting functions that are integral to the operation and control of the service (for example, IT support and human resources) are also considered within the system boundaries. Functions and activities that do not directly or indirectly contribute to the delivery, security, or availability of the service are excluded from the boundaries of the DIS Direct Service.

The subsections below describe the components that support the operation of the DIS Direct Service.

Infrastructure and Software

The Company utilizes Microsoft 365 to provide the resources to provide infrastructure and data hosting services that support the DIS Direct Service. By leveraging the resiliency, scalability, and security features of these infrastructure services, the Company is able to host and operate the DIS Direct Service in a secure and reliable manner that meets current and future demand.

The Company remains responsible for designing, configuring, and maintaining the system architecture within Microsoft 365 to ensure that security, availability, and resiliency requirements are met.

The Company also leverages software components to operate the DIS Direct Service and deliver services to its customers. These include applications, platforms, and supporting tools used to build, secure, monitor, and maintain the environment. The Company remains responsible for selecting, implementing, and maintaining these software components to ensure that applicable system requirements are met.

The in-scope infrastructure and software components are outlined in the table below.

Infrastructure and Software Component	Business Function
Application Firewall (macOS)	Endpoint Firewall
FileVault	Disk Encryption
Microsoft 365	Secure Communication, Collaboration, and Document Management
Microsoft 365 Unified Audit Log	Security Monitoring and Log Management
Microsoft Defender for Endpoint	Anti-malware
SonicWall	Network Traffic Control
XProtect	Anti-malware

People

The Company's personnel are responsible for operating, securing, and supporting the DIS Direct Service. Personnel perform activities necessary to deliver the Company's services, including governance, operations, customer support, and security-related functions. The Company remains responsible for recruiting, training, and overseeing personnel to ensure that their roles are performed in accordance with applicable policies and requirements.

The in-scope personnel roles and responsibilities are outlined in the table below:

Role/Unit Name	Responsibilities
Customer Success	Responsible for managing and strengthening customer relationships to drive adoption, satisfaction, and retention of products and services.
Executive Management	Responsible for providing strategic leadership, overseeing company-wide activities, and ensuring organizational goals and objectives are established, communicated, and achieved.
Sales	Responsible for revenue generation, client acquisition, and management of the sales pipeline.

Procedures

The Company relies on documented automated and manual procedures to govern the operation, security, and support of the DIS Direct Service. These procedures are maintained in alignment with the Company's Information Security Policy and are reviewed and updated as necessary for changes in the business, but no less than annually. The Company remains responsible for developing, implementing, and maintaining these procedures to ensure they are followed consistently and support the Company's operational and compliance objectives.

The in-scope procedures are outlined in the table below:

Procedure	Description
Access Control	How the Company restricts access to its systems and facilities, provisions and removes access rights, and prevents unauthorized access.
Asset Management	How the Company tracks and manages its assets, including hardware and software, to ensure accurate records, compliance with requirements, and protection of resources.
Business Continuity and Disaster Recovery	How the Company identifies the steps to be taken in the event of a disaster to help resume business operations.
Change Management	How the Company identifies, reviews, and implements system changes using a controlled process to prevent unauthorized or untested changes.
Data Classification, Handling, and Retention	How the Company classifies data, establishes requirements for its secure handling and storage, determines retention periods in compliance with requirements, and securely disposes of records when no longer needed.
Incident Management	How the Company detects, reports, responds to, and manages incidents that could affect the operation or protection of the system, in order to minimize impact and support recovery.
Monitoring and Logging	How the Company collects, reviews, and analyzes system activity logs and alerts to detect and respond to unusual or unauthorized activity.
Risk and Vendor Management	How the Company identifies, assesses, and mitigates risks to the system, including risks arising from business disruptions, operations, and the use of vendors and business partners by evaluating, selecting, and monitoring vendors to ensure they meet security and compliance requirements.
Security Awareness and Training	How the Company trains personnel on security and compliance requirements and monitors completion of training activities.
System Operations	How the Company manages and monitors system operations and responds to deviations, including security-related events.

Data

Data refers to transaction streams, files, data stores, tables, and other outputs used or processed by the DIS Direct Service. While the Company maintains data necessary for the operation and support of the DIS Direct Service, customers remain responsible for defining and controlling the data they provide and maintain within the DIS Direct Service. The Company remains responsible for managing and protecting that data in accordance with its policies,

contractual commitments, and applicable regulatory requirements.

Disk encryption is enabled on employee workstations.

System Incidents

A system event is defined as an occurrence that could lead to the loss of, or disruption to, operations, services, or functions and result in DIS Direct's failure to achieve its service commitments or system requirements. Such an occurrence may arise from actual or attempted access or use by internal or external parties and may:

- Impair or potentially impair the availability, integrity, or confidentiality of information or systems.
- Result in unauthorized disclosure or theft of information or other assets, or the destruction or corruption of data.
- Cause damage to systems.

Such occurrences also may arise from the failure of the DIS Direct Service to process data as designed or from the loss, corruption, or destruction of data used by the DIS Direct Service.

On the other hand, a system incident is defined as a system event that requires action on the part of DIS Direct management to prevent or reduce the impact of the event on DIS Direct's achievement of its service commitments and system requirements.

There were no identified significant system incidents that (a) resulted from controls that were not suitably designed or operating effectively to achieve one or more of the service commitments and system requirements, or (b) otherwise resulted in a significant failure in the achievement of one or more of those service commitments and system requirements throughout the period February 1, 2025 to January 31, 2026.

The Applicable Trust Services Criteria and Related Controls

Applicable Trust Services Criteria

The Trust Services Category that is in scope for the purposes of this report is Security.

- **Security:** Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect the entity’s ability to meet its objectives.

The common criteria are organized as follows:

1. **Control Environment:** The criteria relevant to how the entity is structured and the processes the entity has implemented to manage and support people within its operating units. This includes criteria addressing accountability, integrity, ethical values, qualifications of personnel, and the environment in which they function.
2. **Information and Communication:** The criteria relevant to how the entity communicates its policies, processes, procedures, commitments, and requirements to authorized users and other parties of the system and the obligations of those parties and users to the effective operation of the system.
3. **Risk Assessment:** The criteria relevant to how the entity (i) identifies potential risks that would affect the entity’s ability to achieve its objectives, (ii) analyzes those risks, (iii) develops responses to those risks including the design and implementation of controls and other risk mitigating actions, and (iv) conducts ongoing monitoring of risks and the risk management process.
4. **Monitoring Activities:** The criteria relevant to how the entity monitors the system, including the suitability and design and operating effectiveness of the controls, and acts to address deficiencies identified.
5. **Control Activities:** The criteria relevant to the actions established through policies and procedures that help

ensure that management's directives to mitigate risks to the achievement of objectives are carried out.

6. **Logical and Physical Access Controls:** The criteria relevant to how the entity restricts logical and physical access, provides and removes that access, and prevents unauthorized access.
7. **System Operations:** The criteria relevant to how the entity manages the operation of a system and detects and mitigates processing deviations, including logical and physical security deviations.
8. **Change Management:** The criteria relevant to how the entity identifies the need for changes, makes the changes using a controlled change management process, and prevents unauthorized changes from being made.
9. **Risk Mitigation:** The criteria relevant to how the entity identifies, selects, and develops risk mitigation activities arising from potential business disruptions and the use of vendors and business partners.

This report is focused solely on the Security category.

Control Environment

Integrity and Ethical Values

DIS Direct places emphasis on ethics and communication within the organization. Management communicates and oversees the Code of Conduct, which defines expected responsibilities and behavior regarding data and information system usage. All personnel are required, upon hire, to acknowledge in writing that they have received, read, and understood its contents.

DIS Direct demonstrates its commitment to integrity in all interactions with customers, vendors, and personnel by maintaining documented policies that establish ethical and business conduct standards. These policies guide decision-making, reinforce accountability, and support the control environment.

As part of its compliance framework, DIS Direct maintains an inventory of third-party service providers that support the system. These providers are contractually obligated to adhere to information security requirements and to report cybersecurity incidents in a timely manner, ensuring that vendor practices align with DIS Direct's integrity and security requirements.

Oversight and Authority

The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function. The Risk Committee meets quarterly and maintains formal meeting minutes.

Organizational Structure

DIS Direct's organizational structure provides a framework for planning, executing, and controlling business operations. Roles and responsibilities are formally documented, communicated, and assigned to ensure adequate staffing, operational efficiency, segregation of duties, and oversight of the security and control environment. Management has also established clear authority levels and reporting lines for key personnel to maintain accountability. DIS Direct follows a formal onboarding program to assist new personnel as they become familiar with organizational processes, systems, policies, and procedures. This structure supports alignment of responsibilities with the Company's internal control, compliance, and security objectives.

Management's Philosophy and Operating Style

DIS Direct's management adopts an active and engaged approach to business operations, maintaining close communication with the workforce and key vendor representatives. Management emphasizes ethical conduct,

responsibility, and compliance with established policies across all areas of the organization.

The leadership team is directly involved in setting strategic objectives, overseeing operational activities, and reinforcing the importance of security, confidentiality, and integrity in daily practices. This operating style promotes a culture of transparency, responsiveness, and proactive risk management, ensuring that decisions align with the Company's objectives and requirements.

Authority and Responsibility

DIS Direct assigns appropriate levels of authority and responsibility to personnel across the organization to facilitate effective internal control. Roles and responsibilities are documented and communicated through job descriptions, policies, and procedures to ensure individuals understand their obligations in maintaining security and compliance.

Oversight mechanisms are in place to review and approve critical activities, ensuring that responsibilities are appropriately segregated to reduce the risk of conflicts of interest and unauthorized actions.

Human Resources

All new personnel are subject to pre-employment screening, such as reference or background checks, consistent with the Company's hiring practices, before being granted access to production systems or sensitive data. As part of the onboarding process, personnel are also required to review and sign confidentiality agreements, reinforcing their obligation to safeguard company and customer information and prohibiting unauthorized disclosure of data.

The Company follows a structured onboarding program to familiarize new personnel with security policies, operational processes, and role-specific responsibilities. Information security training is mandatory upon hire and reinforced through annual refresher training to ensure personnel understand the Company's security practices, their role in protecting systems and data, and key concepts such as cybersecurity threats, phishing and social engineering, malware, secure data handling, authentication practices, and incident reporting. Supplemental awareness campaigns and targeted communications are also used to strengthen security awareness throughout the year.

The Company has implemented a performance management process to provide feedback, assess effectiveness, and align individual objectives with organizational goals.

Information and Communication

DIS Direct maintains an Information Security Policy that defines the information security rules and requirements for the service environment. The policy is reviewed and approved by management and communicated to all relevant personnel.

Processes are in place to ensure that critical information related to security, system availability, and compliance objectives is communicated effectively both internally and externally. Management ensures that personnel receive timely updates on new or revised policies, control requirements, and operational procedures through established communication channels such as internal knowledge bases, scheduled briefings, and formal announcements.

The Company maintains documented guidance describing how personnel should escalate incidents, compliance concerns, or process deviations. Communication lines are structured to ensure that information reaches the appropriate decision-makers without unnecessary delay, including mechanisms for reporting control exceptions and protocols for sharing updates with clients and vendors.

To promote transparency with stakeholders, DIS Direct provides documentation describing service features, security practices, and compliance measures. This documentation is reviewed and updated periodically to reflect changes in systems or requirements.

Risk Assessment and Mitigation

DIS Direct maintains a formal risk assessment process to identify, evaluate, and manage risks that could affect its objectives and the delivery of secure, reliable services. Each identified risk is evaluated and rated to ensure that appropriate controls are designed and implemented to mitigate the most significant threats to the Company's systems and operations.

The risk assessment is conducted annually and updated in response to significant changes in technology, operations, regulatory requirements, business strategy, or other emerging risks. This ensures new risks are identified and addressed in a timely manner.

DIS Direct applies a structured methodology that includes:

- Identifying threats – considering internal and external factors such as technology, operations, personnel, vendor dependencies, and regulatory changes.
- Analyzing vulnerabilities – assessing weaknesses in processes, technology, and personnel that could expose the Company to exploitation.
- Estimating likelihood of impact – evaluating the probability that a vulnerability could be successfully exploited.
- Assessing severity of impact – analyzing potential consequences, including operational, financial, reputational, and regulatory implications.
- Ranking and prioritizing risks – combining likelihood and impact ratings to establish a risk score and guide remediation priorities.

Assessment results are reviewed by management and used to inform the design and implementation of controls, security policies, and ongoing risk mitigation activities. Mitigation strategies include implementing preventive and detective controls, monitoring key risk indicators, and formally tracking remediation activities through completion.

The process is integrated into the Company's governance, risk, and compliance (GRC) framework to ensure that risks are continuously identified, evaluated, and addressed in strategic planning and operational decision-making.

Vendor Management

DIS Direct maintains a Vendor Management Policy that governs the selection, onboarding, and ongoing oversight of third-party service providers. The policy includes requirements for classifying vendors based on criticality, assessing risks associated with the procurement of third-party services, and reviewing vendor performance on an ongoing basis.

Formal agreements are established with all critical vendors, and these agreements include commitments applicable to the services provided. To ensure that vendor controls remain effective, DIS Direct obtains and reviews third-party attestation reports or performs a vendor risk assessment on an annual basis. Exceptions or control gaps identified in these reviews are evaluated to determine their potential impact on the DIS Direct Service and addressed through remediation or compensating measures where necessary.

Through these activities, vendor risks are identified, monitored, and mitigated as part of DIS Direct's broader GRC framework.

Monitoring

The systems within the boundary are configured to support continuous monitoring, detection, alerting, and testing for vulnerabilities and threats. Management reviews system alerts promptly and supports monitoring through preventive, detective, and corrective audit logging. Relevant monitoring outputs are shared with executive and management personnel to ensure timely awareness and action.

Vulnerability Management and Testing

DIS Direct maintains a documented Vulnerability Management Policy that defines methods for identifying vulnerabilities, assessing their severity, and prioritizing remediation or mitigation activities within defined timelines. The policy provides the framework for consistent execution of vulnerability management practices.

In alignment with this policy, DIS Direct performs both automated and manual security testing at regular intervals. Workstations supporting the service are patched as a part of routine maintenance to help ensure that workstations supporting the service are hardened against security threats. Identified vulnerabilities are ranked and remediated in accordance with the Company's Vulnerability Management Policy and related procedures.

Threat Monitoring and Logging

The Company employs log management tools to monitor and analyze security events and trends that may impact its ability to achieve security objectives. Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on workstations.

Alerting and Escalation

The Company employs a distributed monitoring approach that combines commercially available tools, custom code, and instant messaging platforms. This system attributes critical security events to their source and sends targeted alerts to authorized personnel with the authority and context necessary to validate them. Alerts are reviewed by authorized personnel, who address them when appropriate or escalate to designated teams for resolution.

Control Activities

DIS Direct has implemented documented policies, procedures, and technical controls to mitigate identified risks and support the Company's objectives and requirements. Control activities are designed and implemented across the organization, embedded into business processes, and aligned with objectives for safeguarding systems and data. These activities include:

- **Governance and Policy Controls** – Documented policies and standards that define responsibilities and expected practices for personnel.
- **Technical and Monitoring Controls** – Safeguards and monitoring mechanisms designed to prevent, detect, and respond to unauthorized or anomalous activity.
- **Operational Controls** – Processes that integrate security and compliance practices into daily operations.
- **Third-Party Oversight Controls** – Oversight of vendors and service providers through contractual requirements, risk assessments, and periodic reviews.

Together, these control activities form a structured framework that mitigates risks to the service and supports the Company's objectives and requirements.

Logical Access

DIS Direct maintains a documented Access Control Policy that defines the requirements for provisioning and deprovisioning users, performing access reviews and recertifications, and restricting access based on separation of duties and least privilege. Access reviews are conducted to confirm that system access remains appropriate and access is modified or removed as necessary. Password configurations for system components are enforced in accordance with DIS Direct's Password Policy.

Access to system components is based on job role and function, and requires a documented request with manager approval prior to provisioning. Users are assigned unique user IDs before being granted access. Access rights are assigned using Role-Based Access Control (RBAC) and the principle of least privilege, ensuring users are granted only the access required for their job duties. Privileged access to system components is restricted to authorized users with a business need, and access to production infrastructure requires valid multi-factor authentication (MFA) tokens. Access to system components is revoked within 24 hours of termination as part of the termination process.

System Operations

DIS Direct maintains a documented Incident Response Policy that establishes a structured process for preparing for, detecting, responding to, and recovering from incidents. The policy also defines requirements for analysis, communication, follow-up, and training to strengthen resilience and improve future response. Personnel responsibilities during a breach, the steps for managing an incident, and the importance of information security awareness are documented and communicated to all personnel.

The Incident Response Team employs industry-standard procedures such as identification, verification, classification, and prioritization to drive effective resolution during business-impacting events. Alerts are reviewed, triaged, and escalated according to severity, ensuring timely involvement of technical and management stakeholders.

Post-mortems are convened after any significant operational issue, regardless of whether external impact occurred. Findings are documented to capture the root cause, identify lessons learned, and track preventative or corrective actions to completion. The incident response plan is tested annually to assess the effectiveness of the incident response program.

Change Management

DIS Direct maintains a documented Change Management Policy to guide the processes for requesting, documenting, reviewing, approving, testing, scheduling, and implementing changes. Changes that may affect system availability, security, or confidentiality are communicated to management and any affected partners.

System configuration standards are documented and implemented to ensure systems and network devices are securely configured. Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.

Secure Software Development: To provide the DIS Direct Service, software and infrastructure are utilized. However, DIS Direct does not develop software or manage infrastructure to support the in-scope services. Microsoft 365 is responsible for the software development and infrastructure change management for the infrastructure and data hosting services provided to DIS Direct.

Complementary User Entity Controls (CUECs)

In designing its controls, DIS Direct management did not identify any CUECs that would be necessary, in combination with controls at DIS Direct, to provide reasonable assurance that its principal service commitments and system requirements would be achieved. Accordingly, no CUECs are required to achieve the service commitments and system requirements based on the applicable trust services criteria.

User Entity Responsibilities

DIS Direct's controls related to the DIS Direct Service are sufficient, in and of themselves, to achieve its principal service commitments and system requirements. Accordingly, no CUECs are required. However, user entities remain responsible for implementing and maintaining their own internal controls to ensure the proper use of the DIS Direct Service within their environments. These responsibilities are intended to support each user entity's broader control environment, ensure the effective use of the services provided, and help user entities derive benefit from those services. The following responsibilities are illustrative and should not be considered a comprehensive listing.

User entities should:

- Report any material changes to their control environment that may impact the services performed by the Company, in accordance with contractually defined time frames.
- Notify the Company of changes to the authorized user list and vendor security requirements.
- Grant access only to authorized and trained personnel and revoke access timely when access is no longer required.
- Maintain physical security and environmental controls at their facilities and for remote workers.
- Implement controls for managing user IDs and passwords used to access the Company's services.
- Notify the Company of any known or suspected security incidents.

Each user entity should assess its own control environment to determine whether additional responsibilities are needed to ensure the effective use of the services and to derive benefit from them.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses Microsoft 365 as a subservice organization. The Company's controls related to the DIS Direct Service cover only a portion of the overall internal control for each user entity of the DIS Direct Service. The description does not extend to the services provided by the subservice organization. Section 4 of this report and the description of the system only cover the Trust Services Criteria and related controls of the Company and exclude the related controls of Microsoft 365.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. Accordingly, CSOCs are expected to be in place at Microsoft 365 as described in the CSOC table below.

Through its operational activities, Company management monitors the services performed by Microsoft 365 to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to Microsoft 365 management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to the DIS Direct Service to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls and related tests and results described in Section 4 of this report, taking into account the related CSOCs expected to be implemented at Microsoft 365 as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	Microsoft 365 is responsible for encrypting customer data at rest and in transit within its platform to mitigate the risk of unauthorized access to sensitive data. Microsoft 365 is responsible for enforcing access controls and identity protections to mitigate the risk of unauthorized access or privilege escalation
CC6.4	Microsoft 365 is responsible for restricting physical access to its data centers through approval and revocation processes, surveillance and access control mechanisms, periodic reviews of access rights, and retention of monitoring records to mitigate the risk of unauthorized access, intrusion, or physical tampering.
CC6.5	Microsoft 365 is responsible for securely decommissioning production assets in its control and ensuring that data is rendered unreadable or unrecoverable through logical deletion, cryptographic erasure, or physical destruction once no longer required, to mitigate the risk of unauthorized recovery of data from retired equipment.
CC6.6	Microsoft 365 is responsible for applying security patches and updates to its platform components as part of routine maintenance to mitigate the risk of vulnerabilities being exploited. Microsoft 365 is responsible for implementing and maintaining network-layer protections and platform-level security controls to mitigate the risk of unauthorized access or data exposure within their hosted environments.
CC7.2	Microsoft 365 is responsible for implementing and maintaining environmental protection measures at its data centers, including fire detection and suppression systems, temperature and humidity controls, uninterruptible power supply (UPS) units, backup power sources, and monitoring of environmental conditions, to mitigate the risk of outages, equipment failure, or data loss due to environmental hazards or power disruptions.
CC8.1	Microsoft 365 is responsible for managing infrastructure and platform changes including updates, releases, and configuration modifications through formal change management processes to mitigate the risk of unauthorized or untested changes impacting system availability, integrity, or functionality. Microsoft 365 is responsible for following secure software development lifecycle (SDLC) practices including code reviews, vulnerability testing, and release controls to mitigate risks associated with insecure application code and features.

Specific Criteria Not Relevant to the System

There were no specific Security Trust Services Criteria as set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022), in AICPA, Trust Services Criteria* that were not relevant to the system as presented in this report.

Significant Changes to the System

There were no changes that are likely to affect report users' understanding of how the DIS Direct Service was used to provide the service from February 1, 2025 to January 31, 2026.

Report Use

The description does not omit or distort information relevant to the DIS Direct Service while acknowledging that the description is prepared to meet the common needs of a broad range of users and may not, therefore, include every aspect of the system that each individual user may consider important to their particular needs.

SECTION 4

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security Category

Trust Services Criteria, Related Controls and Tests of Controls Relevant to the Security Category

This SOC 2 Type 2 Report was prepared in accordance with the AICPA Attestation Standards based on the criteria for a description of a service organization's system set forth in DC Section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022), in AICPA, Description Criteria (description criteria)* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 1, 2025 to January 31, 2026.

Description of Testing Procedures Performed

Thoropass Assurance evaluated the design and operating effectiveness of the controls listed in this section throughout the period February 1, 2025 to January 31, 2026. Our evaluation included procedures we considered necessary in the circumstances to determine whether the control activities were suitably designed and operating to achieve the service commitments and system requirements based on the relevant trust services criteria throughout the period February 1, 2025 to January 31, 2026.

In determining the nature, timing, and extent of procedures performed, we considered the following factors:

- The nature and timing of the controls being tested.
- The types of evidential matter.
- The appropriateness of the control design and operation relative to the applicable trust services criteria.
- The assessed level of control risk.
- The entity's control environment and related governance processes.

The procedures performed included:

- **Inquiry:** Conducted detailed interviews with relevant stakeholders to obtain evidence that the control operated during the period. This procedure was accompanied by additional testing, as noted below, to corroborate the information obtained through inquiry.
- **Observation:** Observed the performance of the control during the period to obtain evidence of the application of the specific control activity.
- **Inspection:** Inspected relevant documentation, configurations, and reports to obtain evidence that the control activity was designed and operating as intended.
- **Reperformance:** Obtained the documentation used in the performance of the control activity and independently reperformed the control or process to verify its accuracy and operation.

Reliability of Information Produced by DIS Direct

For tests of controls requiring the use of information produced by the entity (IPE) (e.g., controls requiring system-generated populations for sample-based testing), a

combination of the following procedures were performed, where possible, based on the nature of the IPE to address the completeness, accuracy, and data integrity of the data or reports used:

- Inspected the source of the IPE.
- Inspected the query, script, or parameters used to generate the IPE.
- Tied data between the IPE and the source.
- Inspected the IPE for anomalous gaps in sequence or timing to determine the data was complete, accurate, and maintained its integrity.

Furthermore, in addition to the above procedures, for tests of controls requiring management's use of IPE in the execution of controls (e.g., periodic reviews of user access privileges); an inspection of management's procedures, as applicable, to assess the validity of the IPE source and the completeness, accuracy, and integrity of the data or reports was performed. While these procedures were not specifically called out in the test procedures listed in this section, they were completed as a component of our testing to support the evaluation of whether or not the information was sufficiently precise and detailed for purposes of fully testing the controls identified by DIS Direct.

This section of the report includes 2 tables:

Table 1: DIS Direct Controls Mapped to the Security Criteria

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Table 1: DIS Direct Controls Mapped to the Security Criteria

Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.1	REQ-7 REQ-8 REQ-9 REQ-10 REQ-14	The entity demonstrates a commitment to integrity and ethical values.

Control Environment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC1.2	REQ-3 REQ-4	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.
CC1.3	REQ-2 REQ-3 REQ-4 REQ-15 REQ-16	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.
CC1.4	REQ-11 REQ-12 REQ-13 REQ-14 REQ-15	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.
CC1.5	REQ-7 REQ-14 REQ-15	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.

Information and Communication		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC2.1	REQ-4 REQ-19 REQ-20 REQ-33 REQ-39	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.
CC2.2	REQ-2 REQ-13 REQ-15	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.
CC2.3	REQ-5 REQ-6 REQ-22	The entity communicates with external parties regarding matters affecting the functioning of internal control.

Risk Assessment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC3.1	REQ-17 REQ-18	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.

Risk Assessment		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC3.2	REQ-17 REQ-19 REQ-23	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.
CC3.3	REQ-17 REQ-19	The entity considers the potential for fraud in assessing risks to the achievement of objectives.
CC3.4	REQ-17 REQ-19	The entity identifies and assesses changes that could significantly impact the system of internal control.

Monitoring Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC4.1	REQ-4 REQ-19 REQ-20 REQ-23	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.

Monitoring Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC4.2	REQ-4 REQ-19 REQ-20 REQ-23	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.

Control Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC5.1	REQ-17 REQ-20	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.
CC5.2	REQ-17 REQ-20	The entity also selects and develops general control activities over technology to support the achievement of objectives.

Control Activities		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC5.3	REQ-1 REQ-17 REQ-21 REQ-24 REQ-32 REQ-42 REQ-48 REQ-51 REQ-53	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.

Logical and Physical Access Controls		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.1	REQ-24 REQ-25 REQ-26 REQ-27 REQ-33 REQ-34	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.

Logical and Physical Access Controls		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.2	REQ-29 REQ-30 REQ-31	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.
CC6.3	REQ-28 REQ-29	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.
CC6.4	The Company's production environment is hosted at third-party data centers, which have been carved out for the purposes of this report.	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.
CC6.5	REQ-32 REQ-33	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.
CC6.6	REQ-27 REQ-37 REQ-43	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.
CC6.7	REQ-39	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.

Logical and Physical Access Controls		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC6.8	REQ-38 REQ-39 REQ-43	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.

System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.1	REQ-19 REQ-42 REQ-51	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.
CC7.2	REQ-39 REQ-43	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.
CC7.3	REQ-39 REQ-48	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.

System Operations		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC7.4	REQ-43 REQ-48 REQ-49 REQ-50	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.
CC7.5	REQ-48 REQ-49 REQ-58 REQ-59	The entity identifies, develops, and implements activities to recover from identified security incidents.

Change Management		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC8.1	The in-scope service uses Microsoft 365, wherein Microsoft 365 is responsible for software development and infrastructure management, hence this criterion is carved out for purposes of this report.	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.

Risk Mitigation		
Criteria	**Applicable Control Activities**	**Criteria Description**
CC9.1	REQ-17 REQ-48 REQ-49 REQ-58 REQ-59	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.
CC9.2	REQ-21 REQ-22 REQ-23	The entity assesses and manages risks associated with vendors and business partners.

Table 2: Description of Tests of Controls, Service Auditor Tests, and Results of Tests

Control activities and test procedures performed in connection with determining the design and operating effectiveness of controls relative to the applicable Trust Services Criteria are described below.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-1	An Information Security Policy is documented and defines the information security rules and requirements for the service environment. The policy is version controlled, reviewed annually, approved by management, and communicated to authorized users.	Inspected the Information Security Policy and policy repository to determine that an Information Security Policy was documented, defined the information security rules and requirements for the service environment, was version controlled, reviewed annually, approved by management, and communicated to authorized users.	No exceptions noted.
REQ-2	Management has established defined roles and responsibilities to oversee the implementation of the security and control environment.	Inspected the Information Security Policy to determine that management had established defined roles and responsibilities to oversee the implementation of the security and control environment.	No exceptions noted.
REQ-3	The Risk Committee is tasked with governance, oversight, and responsibilities relative to internal control. The Risk Committee includes members that are independent of the internal control function.	Inspected the Risk Committee charter to determine that the Risk Committee was tasked with governance, oversight, and responsibilities relative to internal control and the Risk Committee included members that were independent of the internal control function.	No exceptions noted.
REQ-4	The Risk Committee meets quarterly and maintains formal meeting minutes.	Inspected the Risk Committee meeting minutes for a sample of quarters to determine that the Risk Committee met quarterly and maintained formal meeting minutes.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-5	The Master Service Agreement (MSA) includes the communication of the Company's commitments to its customers.	Inspected the MSA template to determine that the Company's commitments were communicated to customers.	No exceptions noted.
REQ-6	Technical support resources related to system operations are provided on the Company's website.	Inspected the Company's website to determine that technical support resources related to system operations were provided on the Company's website.	No exceptions noted.
REQ-7	The Code of Conduct describes employee responsibilities and expected behavior regarding data and information system usage.	Inspected the Code of Conduct to determine that it described employee responsibilities and expected behavior regarding data and information system usage.	No exceptions noted.
REQ-8	Upon hire, employees acknowledge that they have read and agree to the Code of Conduct.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No new employees were hired during the period. As a result, no operating effectiveness testing could be performed to determine whether employees acknowledged that they had read and agreed to the Code of Conduct upon hire.
REQ-9	The employee confidentiality agreement prohibits any disclosure of information and other data to which the employee has been granted access.	Inspected the employee confidentiality agreement to determine that it prohibited the disclosure of information and other data to which the employee had been granted access.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-10	Upon hire, employees acknowledge that they have read and agree to the confidentiality agreement	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No new employees were hired during the period. As a result, no operating effectiveness testing could be performed to determine whether employees acknowledged that they have read and agreed to the confidentiality agreement upon hire.
REQ-11	New employees offered employment are subject to background checks prior to their start date.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No new employees were hired during the period. As a result, no operating effectiveness testing could be performed to determine whether new employees offered employment were subject to background checks prior to their start date.
REQ-12	New employees complete security awareness training upon hire.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No new employees were hired during the period. As a result, no operating effectiveness testing could be performed to determine whether new employees completed security awareness training upon hire.
REQ-13	Employees complete security awareness training annually.	Inspected the training records for a sample of employees to determine that employees completed security awareness training annually.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-14	Managers complete performance appraisals for direct reports annually.	Inspected the performance appraisals for a sample of employees to determine that managers completed performance appraisals for direct reports annually.	No exceptions noted.
REQ-15	Job descriptions are documented for employees supporting the service and include authorities and responsibilities in support of the system.	Inspected the job descriptions for a sample of employees supporting the service to determine that job descriptions were documented and included authorities and responsibilities in support of the system.	No exceptions noted.
REQ-16	An organization chart is documented and defines the organizational structure and reporting lines.	Inspected the organization chart to determine that an organization chart was documented and defined the organizational structure and reporting lines.	No exceptions noted.
REQ-17	A Risk Management Policy is documented and includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Inspected the Risk Management Policy to determine that a Risk Management Policy was documented and included guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	No exceptions noted.
REQ-18	The Company specifies its objectives in its annual risk assessment to enable the identification and assessment of risk related to the objectives.	Inspected the risk assessment results to determine that the Company specified its objectives in its annual risk assessment to enable the identification and assessment of risks related to the objectives.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-19	A risk assessment is performed annually. As part of this process, threats and changes to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Inspected the risk assessment results to determine that a risk assessment was performed annually and, as part of this process, threats and changes to service commitments were identified, risks were formally assessed, and the risk assessment included a consideration of the potential for fraud and how fraud may have impacted the achievement of objectives.	No exceptions noted.
REQ-20	As part of its annual risk assessment, management selects and develops manual and IT general control activities that contribute to the mitigation of identified risks.	Inspected the risk assessment results to determine that as part of its annual risk assessment, management selected and developed manual and IT general control activities that contributed to the mitigation of identified risks.	No exceptions noted.
REQ-21	A Vendor Management Policy is documented and includes guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	Inspected the Vendor Management Policy to determine that a Vendor Management Policy was documented and included guidance on performing the following vendor management functions: - Requirements for the classification of third-party vendors - Requirements for the assessment of risks resulting from the procurement of third-party services - Annually reviewing critical third-party attestation reports or performing a vendor risk assessment	No exceptions noted.
REQ-22	Formal agreements are in place with critical vendors. These agreements include commitments applicable to that entity.	Inspected the contracts for a sample of critical vendors to determine that formal agreements were in place with critical vendors and the agreements included commitments applicable to that entity.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-23	A third-party attestation report is reviewed annually for all critical vendors. Exceptions noted in the reports are evaluated to determine their impact on the service.	Inspected the third-party attestation report review results for a sample of critical vendors to determine that a third-party attestation report was reviewed annually for all critical vendors and exceptions noted in the reports were evaluated to determine their impact on the service.	No exceptions noted.
REQ-24	An Access Control Policy is documented and includes guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	Inspected the Access Control Policy to determine that an Access Control Policy was documented and included guidance for performing the following system access control functions: - Provisioning users - Deprovisioning users - Access reviews and recertification - Restricting access based on separation of duties and least privilege	No exceptions noted.
REQ-25	Authentication to Microsoft 365 requires a unique username and password.	Inspected the system configurations and observed login attempts to determine that authentication to Microsoft 365 required a unique username and password.	No exceptions noted.
REQ-26	Passwords for Microsoft 365 are configured according to the Password Policy.	Inspected the Password Policy and compared to Microsoft 365 password configurations to determine that passwords for Microsoft 365 were configured according to the Password Policy.	No exceptions noted.
REQ-27	Access to Microsoft 365 is restricted to authorized users with valid MFA tokens.	Inspected the MFA configurations to determine that access to Microsoft 365 was restricted to authorized users with valid MFA tokens.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-28	Privileged access to Microsoft 365 is restricted to authorized users with a business need.	Inspected the system access listings, inquired of management, and compared each user's access privileges to their job role to determine that privileged access to Microsoft 365 was restricted to authorized users with a business need.	No exceptions noted.
REQ-29	Quarterly access reviews are conducted to help ensure that access to Microsoft 365 is restricted appropriately. The review is documented, and access is modified or removed where applicable.	Inspected the access review results for a sample of quarters to determine that quarterly access reviews were conducted to help ensure that access to Microsoft 365 was restricted appropriately, the review was documented, and access was modified or removed where applicable.	No exceptions noted.
REQ-30	Access to system components is based on job role, function, and requires a documented access request with manager approval prior to access being provisioned.	Inquired of management and inspected the system access listings to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No users were provisioned access to the in-scope system components during the period. As a result, no operating effectiveness testing could be performed to determine whether access to system components was based on job role, function, and required a documented access request with manager approval prior to access being provisioned.
REQ-31	Access to system components is revoked within 24 hours of termination as part of the termination process.	Inquired of management and inspected the employee listing to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No terminations occurred during the period. As a result, no operating effectiveness testing could be performed to determine whether access to system components was revoked within 24 hours of termination as part of the termination process.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-32	A Data Retention and Disposal Policy is documented and includes guidance for the secure retention and disposal of customer data.	Inspected the Data Retention and Disposal Policy to determine that a Data Retention and Disposal Policy was documented and included guidance for the secure retention and disposal of customer data.	No exceptions noted.
REQ-33	An inventory of production system assets is maintained by management.	Inspected the production system asset inventory to determine that an inventory of production system assets was maintained by management.	No exceptions noted.
REQ-34	Disk encryption is enabled on employee workstations.	Inspected the encryption configurations for a sample of employee workstations to determine that disk encryption was enabled on employee workstations.	No exceptions noted.
REQ-37	Firewalls are used and configured on the workstations of employees supporting the service to prevent unauthorized access to the environment.	Inspected the firewall configurations for a sample of employee workstations to determine that firewalls were used and configured on the workstations of employees supporting the service to prevent unauthorized access to the environment.	No exceptions noted.
REQ-38	Anti-malware technology is deployed for environments commonly susceptible to malicious attacks and is configured to be updated routinely, logged, and installed on workstations.	Inspected the anti-malware software configurations for a sample of employee workstations to determine that anti-malware technology was deployed for environments commonly susceptible to malicious attacks and was configured to be updated routinely, logged, and installed on workstations.	No exceptions noted.
REQ-39	A log management tool is utilized to monitor and identify security events and trends that may have a potential impact on the Company's ability to achieve its security objectives and generates alerts when security events occur.	Inspected the log management tool dashboard, configurations, and an example alert notification to determine that a log management tool was utilized to monitor and identify security events and trends that may have had a potential impact on the Company's ability to achieve its security objectives and generated alerts when security events occurred.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-42	A Vulnerability Management Policy is documented and includes guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	Inspected the Vulnerability Management Policy to determine that a Vulnerability Management Policy was documented and included guidance for performing the following vulnerability management functions: - Methods for identifying vulnerabilities and frequency - Assessing the severity of identified vulnerabilities - Prioritizing and implementing remediation or mitigation activities for identified vulnerabilities based on severity and defined timelines	No exceptions noted.
REQ-43	Workstations supporting the service are patched as a part of routine maintenance to help ensure that workstations supporting the service are hardened against security threats.	Inspected the workstation configurations for a sample of employee workstations to determine that workstations supporting the service were patched as a part of routine maintenance to help ensure that workstations supporting the service were hardened against security threats.	No exceptions noted.
REQ-48	An Incident Response Policy is documented and includes guidance for detecting, responding to, and recovering from security events and incidents.	Inspected the Incident Response Policy to determine that an Incident Response Policy was documented and included guidance for detecting, responding to, and recovering from security events and incidents.	No exceptions noted.
REQ-49	The incident response plan is tested annually to assess the effectiveness of the incident response program.	Inspected the incident response plan test results to determine that the incident response plan was tested annually to assess the effectiveness of the incident response program.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-50	All incidents related to security are logged, tracked, evaluated, and communicated to affected parties by management until the Company has recovered from the incidents.	Inquired of management and inspected the security incident repository to determine that the circumstances that warrant the operation of the control did not occur during the period.	Not tested. No security incidents occurred during the period. As a result, no operating effectiveness testing could be performed to determine whether all incidents related to security were logged, tracked, evaluated, and communicated to affected parties by management until the Company had recovered from the incidents.
REQ-51	Hardening standards are documented and include guidance on baseline security requirements for production systems before deployment to the production environment.	Inspected the hardening standards to determine that hardening standards were documented and included guidance on baseline security requirements for production systems before deployment to the production environment.	No exceptions noted.
REQ-53	A Change Management Policy is documented and includes guidance for documenting, testing, reviewing, and approving changes to information systems.	Inspected the Change Management Policy to determine that a Change Management Policy was documented and included guidance for documenting, testing, reviewing, and approving changes to information systems.	No exceptions noted.
REQ-58	A business continuity and disaster recovery (BC/DR) plan is documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	Inspected the BC/DR plan to determine that a BC/DR plan was documented to support continuity and recovery of critical services and business processes after unexpected business interruptions.	No exceptions noted.

Control #	Applicable Control Activities	Service Auditor's Tests	Results of Tests
REQ-59	The BC/DR plan is tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	Inspected the BC/DR plan test results to determine that the BC/DR plan was tested annually to assess the effectiveness of management's readiness to respond to unexpected business interruptions.	No exceptions noted.