Insight Assurance

SOC 2 | ISO 27001 | PCI | HIPAA

System and Organization Controls Report (SOC 2® Type 2)

Report on Mirlin Technologies Inc.'s Description of Its Mirlin Connect Services System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security Throughout the Period July 1, 2024 to September 30, 2024

MIRLIN™

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Mirlin Technologies Inc.

Scope

We have examined Mirlin Technologies Inc.'s ("Mirlin Technologies" or "the Service Organization") description of its Mirlin Connect Services System found in Section 3 titled "Mirlin Technologies Inc.'s description of its Mirlin Connect Services System" throughout the period July 1, 2024 to September 30, 2024 ("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 July 1, 2024 to September 30, 2024, to provide reasonable assurance that Mirlin Technologies' 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*.

Mirlin Technologies uses Microsoft Azure (Azure) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Mirlin Technologies, to achieve Mirlin Technologies' service commitments and system requirements based on the applicable trust services criteria. The description presents Mirlin Technologies' controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Mirlin Technologies' 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.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Mirlin Technologies, to achieve Mirlin Technologies' service commitments and system requirements based on the applicable trust services criteria. The description presents Mirlin Technologies' controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Mirlin Technologies' controls. Our examination did not include such complementary user entity controls, and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

Mirlin Technologies is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Mirlin Technologies' service commitments and system requirements were achieved. In Section 2, Mirlin Technologies has provided the accompanying assertion titled "Mirlin Technologies Inc.'s Management Assertion" (assertion) about the description and the suitability of the design and operating effectiveness of controls stated therein. Mirlin Technologies 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 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 operated 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.

We are required to be independent and meet our other ethical responsibilities in accordance with ethical requirements relating to the examination engagement.

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

- 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.

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 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 Test of Controls

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

Emphasis of Matter – Controls Did Not Operate During the Period Covered by the Report

The Service Organization's description of its system discusses its policies and procedures which include the controls related to the new employees' commitment to integrity and ethical values. However, during the period July 1, 2024 to September 30, 2024, the Service Organization does not have new employees that would warrant the operation of the human resource security procedures. Because those controls did not operate during the period, we were unable to test, and did not test, the operating effectiveness of those controls as evaluated using trust services criteria CC1.1, *The entity demonstrates a commitment to integrity and ethical values*.

Our opinion is not modified with respect to the matter emphasized.

Opinion

In our opinion, in all material respects,

- the description presents Mirlin Technologies' Connect Services System that was designed and implemented throughout the period July 1, 2024 to September 30, 2024, in accordance with the description criteria.

- the controls stated in the description were suitably designed throughout the period July 1, 2024 to September 30, 2024, to provide reasonable assurance that Mirlin Technologies' 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 and user entities applied the complementary controls assumed in the design of Mirlin Technologies' controls throughout that period.
- the controls stated in the description operated effectively throughout the period July 1, 2024 to September 30, 2024, to provide reasonable assurance that Mirlin Technologies' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and user entity controls assumed in the design of Mirlin Technologies' controls operated effectively throughout that period.

Restricted Use

This report is intended solely for the information and use of Mirlin Technologies, user entities of Mirlin Technologies' Connect Services System throughout the period July 1, 2024 to September 30, 2024, and business partners of Mirlin Technologies subject to risks arising from interactions with the Mirlin Connect Services System, 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, and other parties.
- Internal control and its limitations.
- Complementary user entity controls and 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 the specified parties.

Insight Assurance LLC

Tampa, Florida
November 13, 2024

SECTION 2: MIRLIN TECHNOLOGIES INC.'S MANAGEMENT ASSERTION

MIRLIN™

MIRLIN TECHNOLOGIES INC.'S MANAGEMENT ASSERTION

We have prepared the description of Mirlin Technologies Inc.'s ("Mirlin Technologies" or "the Service Organization") Mirlin Connect Services System entitled "Mirlin Technologies Inc.'s description of its Mirlin Connect Services System" throughout the period July 1, 2024 to September 30, 2024 ("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 Mirlin Connect Services System that may be useful when assessing the risks arising from interactions with Mirlin Technologies' system, particularly information about system controls that Mirlin Technologies 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*.

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

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Mirlin Technologies, to achieve Mirlin Technologies' service commitments and system requirements based on the applicable trust services criteria. The description presents the subservice organization controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Mirlin Technologies' controls.

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

- the description presents Mirlin Technologies' Connect Services System that was designed and implemented throughout the period July 1, 2024 to September 30, 2024, in accordance with the description criteria.

- the controls stated in the description were suitably designed throughout the period July 1, 2024 to September 30, 2024, to provide reasonable assurance that Mirlin Technologies' service commitments and system requirements would be achieved based on the applicable trust services criteria, and if the subservice organization and user entities applied the complementary controls assumed in the design of Mirlin Technologies' controls.
- the controls stated in the description operated effectively throughout the period July 1, 2024 to September 30, 2024, to provide reasonable assurance that Mirlin Technologies' service commitments and system requirements were achieved based on the applicable trust services criteria if complementary subservice organization controls and complementary user entity controls assumed in the design of Mirlin Technologies' controls operated effectively throughout that period.

Mirlin Technologies Inc.
November 13, 2024

SECTION 3: MIRLIN TECHNOLOGIES INC.'S DESCRIPTION OF ITS MIRLIN CONNECT SERVICES SYSTEM

MIRLIN TECHNOLOGIES INC.'S DESCRIPTION OF ITS MIRLIN CONNECT SERVICES SYSTEM

Company Background

Mirlin Technologies Inc. ("Mirlin Technologies" or "the company") is a privately held company established in May 2023 offers Mirlin Connect Fleet Management and Maintenance Services ("Mirlin Connect") System. Mirlin Technologies is a Corporation (LLC, Corporation, etc.) headquartered in Mississauga, Ontario, Canada.

Description of Services Overview

Mirlin Technologies understands the challenges of running a fleet, the New Era of fleet management will help customers eliminate waste, downtime and redundancy. Mirlin's ecosystem empowers fleets, service providers, and OEMs to work together seamlessly and efficiently to meet customer needs. With this platform, customers will be able to streamline processes, simplify workflows, and gain valuable insights to increase service automation across the lifecycle of every asset in customer's operation. Mirlin's focus on interpreting complex data sources in a meaningful way means customers will be able to manage, maintain, and service commercial assets with ease and accuracy.

Mirlin Connect is Mirlin Technologies' end-to-end communications services system designed to streamline and optimize fleet management operations. It connects teams with drivers, vendors, and suppliers to enhance productivity, reduce waste, and facilitate smart decision-making for easier and more efficient workflow and automation processes. Mirlin Connect eliminates the need for emails, text messages, and even phone calls with its ability to send messages, photos, attachments, and more.

Some key features include:

- *Centralized Communications:* Integrates multiple communications and brings employees, customers, vendors, and suppliers together into one platform, eliminating the need to juggle multiple tools and suppliers' websites. From service requests to task management, all communications and connections are automated with test completion KPIs and dashboards.
- *Real-time Task Dashboards:* Provides insights into task completion times and statuses, helping to drive accountability, track individual and team performance, and optimize fleet utilization and uptime.
- *Configurable Automated Processes:* By focusing on daily value task workflow automation, Mirlin Connect allows customers to focus on high strategic tasks to optimize the management of their fleet.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Mirlin Technologies designs its processes and procedures related to the Mirlin Technologies' Mirlin Connect Services System ("System") to meet its objectives. Those objectives are based on the service commitments that Mirlin Technologies makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Mirlin Technologies has established for the services.

Security commitments to user entities are documented and communicated in Privacy Policy and Terms of Use.

Security commitments are standardized and include, but are not limited to, the following:

- Comprehensive set of documented and operationalized information security policies.
- System features and configuration settings are designed to authorize user access while restricting unauthorized users from accessing information not needed for their role.
- Use of web application firewall (WAF) and cloud-native application protection platform (CNAPP) to protect and to continuously assess resources against security standards and assist finding weak spots in cloud configurations in order to prevent and identify potential security risks from users outside the boundaries of the system.
- Continuous vulnerability analysis based on CNAPP solution together with annual penetration tests over the production environment.
- Operational procedures for managing security incidents and breaches, including notification procedures.
- Robust access control with strong password policy and multi-factor authentication (MFA)
- Use of encryption technologies to protect customer data both at rest and in transit.
- Use of data retention and data disposal.

Mirlin Technologies establishes operational requirements that support the achievement of security, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.

COMPONENTS OF THE SYSTEM USED TO PROVIDE THE SERVICES

The System description is comprised of the following components:

- ***Infrastructure*** – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT, and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.

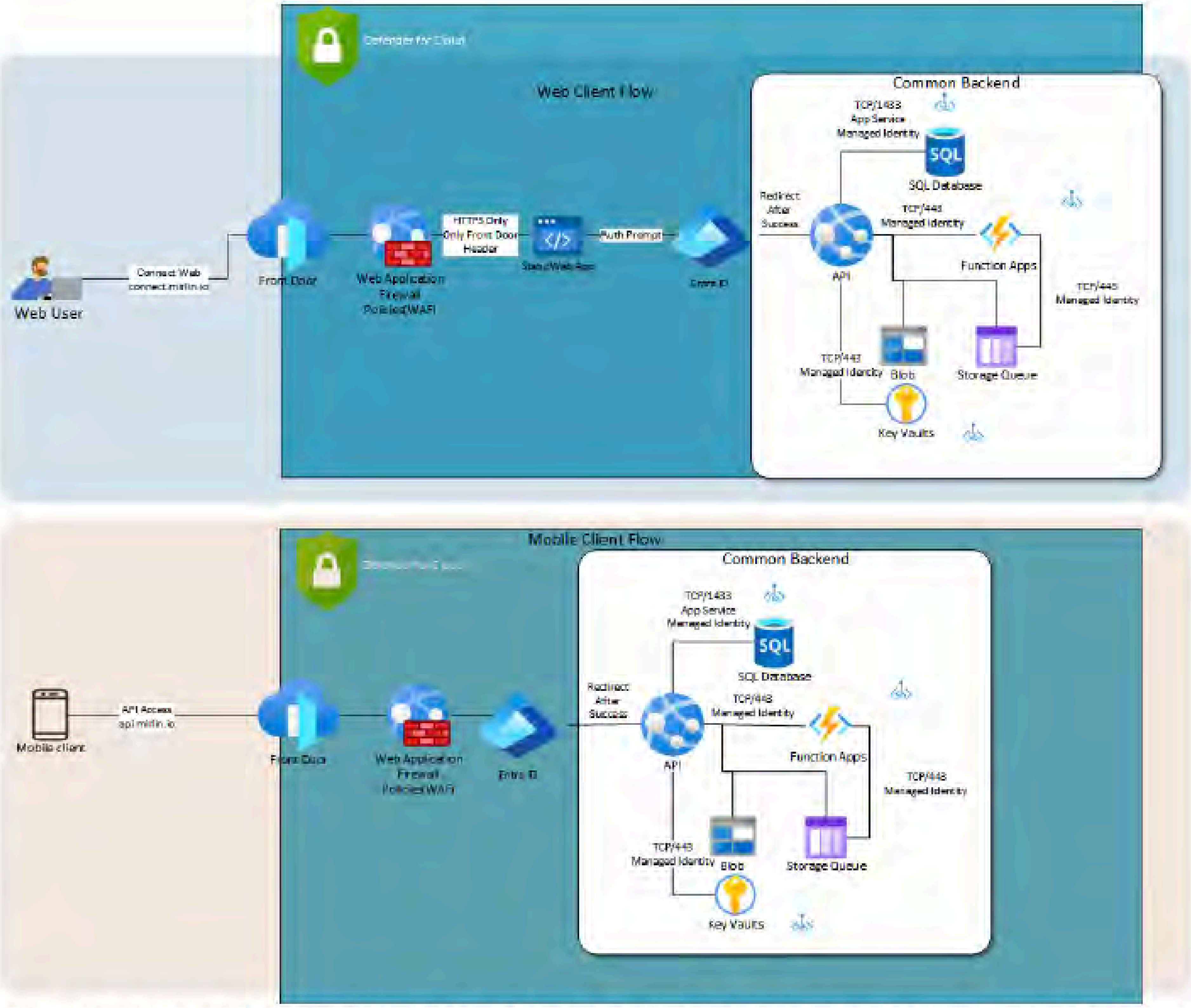
- ***Software*** – The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use mobile applications or desktop or laptop applications are.
- ***People*** – The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- ***Data*** – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- ***Procedures*** – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

Mirlin Technologies' Mirlin Connect Services System production environment infrastructure is implemented at Azure Canada East and Central Regions. In this Azure infrastructure, Mirlin Connect Services System leverages various cloud native services without leveraging virtual machine (VM) to enable the solution to be operated in the cloud efficiently and securely. Mirlin Technologies maintains a system inventory that includes Azure Virtual Networks, databases, storage, and enduser computers (desktops and laptops). The inventory documents device name, device type, description, provider/source, owner, and notes. In-scope infrastructure components are shown in the table below:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
Azure Platform	Platform	Managed cloud platform where services are hosted.
Azure SQL	Database	Transactional database that contains customer information with backups and redundancy.
Azure Web Application Firewall (WAF)	Networking	Used to protect Mirlin Connect application from common web vulnerabilities and attacks.
Azure Front Door	Networking	Acts as a scalable and secure entry point for Mirlin Connect Services System. It provides improved performance, scalabilitiy, reliability and security.
Azure Blob Storage	Storage	Used to store large amounts of unstructured data.
Azure Monitor	DevOps	Monitoring solutions for the cloud environment by gathering data (metrics, logs, etc) from Azure resources, and provides analytics / insights together with alerts / notifications for a timely response to issues that arise.

To outline the topology of its network, the organization maintains the following network diagram:



The subservice organization provides the physical security and environmental protection controls, as well as managed services for Mirlin Technologies' infrastructure.

In addition to the web application firewall, Mirlin Connect's infrastructure includes cloud-native application protection platform (CNAPP) to protect and to continuously assess resources against security standards and assist in finding weak spots in cloud configurations in order to prevent and identify potential security risks from users outside the boundaries of the system. Furthermore, Mirlin Technologies uses endpoint detection and response (EDR) solution on their endpoints to continuously monitor and protect systems from commonly known and unknown threats and malware.

Mirlin Technologies' information security policy governance ensures that all computer devices (including servers, desktops, printers, etc.) connected to the Mirlin Technologies network have proper virus / malware protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department, together with 24x7x365 SOC team, verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the EDR solution will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans, together with penetration testing, are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and data. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Mirlin Technologies-owned computers as employees do not have local administrative rights to their systems. IT staff maintain several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

SOFTWARE

Mirlin Technologies is responsible for managing the development and operation of Mirlin Connect Services System including infrastructure components such as Azure's networking, databases, and storage services. In addition to the above infrastructure components, the in-scope Mirlin Technologies software components are shown in the table provided below:

Primary Software	
Application	**Purpose**
Azure SDK	The SDK is used to communicate with Azure web services.
Microsoft Defender for Cloud	CNAPP solution deployed in the cloud to protect cloud resources. It has various capabilities, including Cloud Security Posture Management (CSPM), Cloud Workload Protection (CWP), Integrated Security Monitoring and Policy Management, and Threat Protection that provides protection of critical workloads across various Azure services / resources.
Microsoft Defender for Endpoints	Endpoint Security Solution deployed across all endpoints (workstations / laptops).
Microsoft Entra ID	Identity and Access Management to the cloud infrastructure.
Azure Key Vault	This Azure service / application is used to store and manage cryptographic keys and secrets securely.
Microsoft Endpoint Manager (Intune)	Manages the Endpoint systems/mobile devices
Microsoft 365	Allow the User Management
Drata	GRC tool to utilize data security, auditing, and information security control management.
Mirlin Connect	Manages the ticketing system.

PEOPLE

Mirlin Technologies is a private corporation located in Mississauga, Ontario. There are an estimated 13 employees organized into various areas of responsibilities, including but not limited to Sales, Operations, Finance, Human Resources, and Information Technologies.

At Mirlin Technologies, the Chief Technology Officer (CTO) is responsible for the technological direction and advancements of the organization. The CTO directs operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the Mirlin Technologies customer base using the service.

Under the CTO, there is a dedicated Software & DevOps Engineering team that focuses on the development Mirlin Connect, and a Product Management team that focuses on the infrastructure support with its Support Engineer team. This support engineering team is responsible for managing day-to-day systems and network operations, as well as managing information security, including but not limited to reviewing vulnerability assessments, with the support from CTO, 24x7x365 SOC team, third-party cybersecurity consultants, and other management team members from Software & DevOps Engineering and Product Management teams. Furthermore, the Support Engineer team handles incident tickets and the change management process.

Staff provide support to the above services. Mirlin Technologies employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. Mirlin Technologies focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep Mirlin Technologies and its data secure.

DATA

Data is categorized into the following major types of data used by Mirlin Technologies:

Data		
Category	**Description**	**Examples**
Public	• Information that has been approved for release to the general public • Freely shareable both internally and externally	• Press releases • Public website
Internal	• Non-sensitive Information • Originating within or owned by Mirlin Technologies or entrusted to it by others. • May be shared with authorized employees, contractors, and business partners who have a business need, but may not be released to the general public, due to the negative impact it might have on the company's business interests	• Internal memos • Policies • Design documents • Product specifications • Correspondences
Confidential	• Sensitive information	• Customer operating data

Data		
Category	**Description**	**Examples**
	• Level of protection is dictated internally by Mirlin Technologies. • Must be limited to only authorized employees, contractors, and business partners with a specific business need	• Customer PII • Customers' customers' PII / PHI • Anything subject to a confidentiality agreement with a customer
Restricted	• Highly sensitive information • Level of protection is dictated externally by legal and/or contractual requirements • Must be limited to only authorized employees, contractors, and business partners with a specific business need.	• Legal documents • Contractual agreements • Employee PII • Employee salaries

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by Mirlin Technologies in delivering its Mirlin Connect services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed or written on paper, and spoken in conversations. All employees and contractors of Mirlin Technologies are obligated to respect and, in all cases, to protect confidential and restricted data, which includes customer data.

The IT department is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Mirlin Technologies has policies in place to ensure prior retention and disposal of confidential and restricted data. The data protection and retention policies define the retention periods and proper destruction requirements for disposing data. These policies are reviewed at least annually. Customer data enters an expired state when the account is voluntarily closed. Expired account data will be retained for 90 days. After this period, the account and related data will be removed. Stored Sensitive data, such as the customer data, that is no longer required will be properly deleted in accordance with Mirlin Technologies' business objectives, applicable laws and regulations, and relevant third-party agreements. A record of such deletion will be kept.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Mirlin Connect's production network is protected by enterprise-class security protection is in place. Password protection, together with multifactor authentication (MFA), with assigned user rights is required for access to the Mirlin Connect's production network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, integrity and availability for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization's intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Physical Security and Environmental Controls

Mirlin Connect production environment is maintained by Azure. Physical and environmental security protections are the responsibility of Azure. Mirlin Technologies reviews the attestation reports and performs a risk analysis of Azure on at least an annual basis.

Logical Access

Mirlin Technologies provides employees and contracts access to infrastructure via a role-based access control system, to ensure uniform, least privileged access to identified users and to maintain simple and reportable user provisioning and de-provisioning processes.

Mirlin Technologies, together with its third-party cloud management service provider, handles the administrative responsibilities involved in supporting the web, application, and database components of Mirlin Connect Services System. To do this, administrators need to authenticate on Azure portal that leverages strong passwords with multifactor authentication (MFA). Access to it is controlled by Microsoft Entra ID and conditional access. Logical access to Mirlin Technologies' networks, applications, and data is limited to properly authorized individuals.

Change Management

For internally developed software platforms/solutions, Mirlin Technologies uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before the final release. All software development activities follow the internal project-related business process model.

Mirlin Technologies has a Change Management Policy in place to control information resources that require an outage for planned upgrades, maintenance, or fine-tuning. Additionally, unplanned outages may occur that may result in upgrades, maintenance, or fine-tuning. The purpose of the Change Management Policy is to manage changes in a rational and predictable manner so that staff and clients can plan accordingly. Changes require forethought, monitoring, and follow-up evaluation to reduce negative impact on the user community and to increase the value of Information Resources.

Computer Operations

Mirlin Technologies maintains an incident response plan to guide employees on reporting and responding to any information security events or incidents. Procedures are in place for identifying, reporting, and acting upon breaches or other incidents.

Mirlin Technologies internally monitors all applications, including web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Mirlin Technologies utilizes Microsoft Defender for Cloud to check common security issues as well as for vulnerabilities identified in its Mirlin Connect environment and maintains an internal SLA for responding to those issues.

Data Communications

Mirlin Technologies has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies Mirlin Technologies logical network configuration by providing an effective firewall around all Mirlin Technologies application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.
The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Patch Management

Mirlin Technologies takes a proactive approach to patch management. Mirlin Technologies leverage Microsoft Defender for Cloud that continuously monitors Mirlin Connect's environment and provides a list of findings that need to be addressed. In addition, the CTO and engineers regularly monitor various websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. This allows the company to plan for upcoming patches.

The engineering team reviews the availability of patches and independently determines if deployment within the production environment is necessary and how soon, depending on the critical nature of the patches. Approved patches are scheduled for installation in the test environment as applicable. If there are no issues in the test environment, the patch will be applied to the production environment. The patching process is tracked via the ticketing system.

Backup and Recovery

Mirlin Technologies performs automatic backups of all customer and system data to protect against catastrophic loss due to unforeseen events that impact the entire system. An automated process backs up all data to a separate Azure region. By default, data will be backed up daily and are encrypted at rest and in-transit. Backups are monitored and alerted by Azure Monitor for a timely review and remediation in case backups fail.

Problem Management

Mirlin Technologies maintains an Incident Response Plan that describes the process for identifying and addressing potential security incidents. The plan details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization conducts Incident Response tabletop exercise annually and provides formal security breach training.

The organization provides a customer service request form where Mirlin Technologies can report potential security breaches, and Mirlin Technologies also provides an email and phone number for this same purpose. Internal users are directed to report incidents via email or through their reporting lines for documentation and tracking purposes.

System Monitoring

The Data Protection Policy and Vulnerability Management Policy describe the organization's policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation.

The organization uses Azure Monitor for system logging within the Azure environment, and this monitors both capacity and performance monitoring of Mirlin Connect Services System.

Azure Web Application Firewall (WAF) and Defender for Cloud are used for threat detection purposes, and these tools generate security event logs for intrusion detection.

Combining Microsoft Defender for Cloud with annual technical vulnerability assessments and penetration tests creates a robust security monitoring framework. This combination offers:

- *Continuous Monitoring*: Defender for Cloud provides ongoing surveillance, while annual assessments and penetration tests offer periodic deep dives into Mirlin Connect security posture.
- *Holistic View*: Combining automated tools with manual testing ensures that both common and complex vulnerabilities are identified and addressed in a timely manner.

- *Proactive Defense*: Regular assessments and testing help in proactively identifying and mitigating risks before they can be exploited by attackers.

The organization uses Microsoft Endpoint Manager for computer monitoring and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least three months and are readily available.

Mirlin Technologies has also engaged a 24x7x365 by third-party Security Operations Center (SOC) service provider that uses a SIEM solution for security event logging and monitoring of security incidents.

Vendor Management

The organization maintains a Vendor Management Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendors' cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Boundaries of the System

The boundaries of the Mirlin Connect Services System are the specific aspects of the Mirlin Technologies' infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Mirlin Connect Services System.

This report does not include the Cloud Hosting Services provided by Azure at multiple facilities.

RELEVANT ASPECTS OF THE CONTROL ENVIRONMENT, RISK ASSESSMENT PROCESS, CONTROL ACTIVITIES, INFORMATION AND COMMUNICATION, AND MONITORING

The Security category, and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Security criteria and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section 4 of this report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of Mirlin Technologies' description of its system.

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement and ensure effective operational controls. The senior management establishes the tone at the top regarding the importance of internal control and expected standards of conduct.

Management Philosophy, Integrity, and Ethical Values

Mirlin Technologies' control of the environment reflects the philosophy of senior management concerning the importance of the security of data. Integrity and ethical values are essential elements of Mirlin Technologies' control environment. Management is responsible for setting the tone at the top, establishing, communicating, and monitoring control policies and procedures.

Formal policies, and Code of Conduct are documented and communicated to employees to ensure that entity values, ethics, integrity, and behavioral standards are a primary focus, and risks are mitigated in daily operations. In addition, a sanctions policy is in place to address deviations from established security and personnel standards.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Mirlin Technologies place a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under Mirlin Technologies' policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security. Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Commitment to Competence

Mirlin Technologies has standardized human resource policies and procedures. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization.

Training and development opportunities are provided to staff and performance evaluations are performed to communicate goals based on job responsibilities and address any performance issues.

Employees are trained in their specific roles and policies through on-the-job training and procedures are reviewed. Management communicates any changes to these policies on an ongoing basis and policies are updated as needed. In order to protect confidential intemal and client information employees are prohibited from divulging any information regarding client affairs or taking action, not in the interests of the client or Mirlin Technologies.

Specific control activities that the service organization has implemented in this area are described below:

- Management has considered the competence levels for jobs and translated required skills and knowledge levels into written position requirements.
- Training is provided to maintain the skill level of personnel in certain positions.

Organizational Structure and Assignment of Authority and Responsibility

Mirlin Technologies' organizational structure provides the framework within which its activities for achieving entity-wide objectives are planned, executed, controlled, and monitored. Management believes establishing a relevant organizational structure includes considering key areas of authority and responsibility. An organizational structure has been developed to suit its needs. This organizational structure is based, in part, on its size and the nature of its activities.

Mirlin Technologies' assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring 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.

Specific control activities that the service organization has implemented in this area are described below:

- Organizational charts are in place to communicate key areas of authority and responsibility.
- Organizational charts are communicated to employees and updated as needed.

Human Resources Policies and Procedures

Mirlin Technologies' success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensure the service organization operates at maximum efficiency. Mirlin Technologies' human resources policies and practices relate to employee hiring, orientation, training, evaluation, counseling, promotion, compensation, and disciplinary activities.

Specific control activities that the service organization has implemented in this area are described below:

- New employees are required to sign acknowledgment forms for the Code of Conduct and a confidentiality agreement following new hire orientation.
- Evaluations for each employee are performed on an annual basis.
- Employee termination procedures are in place to guide the termination process.

RISK ASSESSMENT PROCESS

Mirlin Technologies' risk assessment process identifies and manages risks that could potentially affect Mirlin Technologies' ability to provide reliable and secure services to the company's customers. As part of this process, Mirlin Technologies maintains a risk register to track all systems and procedures that could present risks to meeting the company's objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is re-evaluated at least on an annual basis, and tasks are incorporated into the regular Mirlin Technologies' product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Mirlin Technologies' system; as well as the nature of the components of the system result in risks that the criteria will not be met. Mirlin Technologies addresses these risks through the implementation of suitable-designed controls to provide reasonable assurance that the criteria are met. Because each system and the environment in which it operates are unique, the combination of risks to meeting the criteria and the controls necessary to address the risks will be unique. As part of the design and operation of the system, Mirlin Technologies' management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

INFORMATION AND COMMUNICATION SYSTEM

Information and communication are an integral component of Mirlin Technologies' internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations. Therefore, Mirlin Technologies has an information security policy to help ensure that employees understand their roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner.

Mirlin Technologies uses several information and communication channels internally to share information with management, employees, contractors, and customers. Mirlin Technologies uses chat systems and email as the primary internal and external communications channels.

Additional communication methods include department meetings to communicate company policies, procedures, industry or business issues, or other topics management deems key to the achievement of the organization's objectives. Communication is encouraged at all levels to promote the operating efficiency of Mirlin Technologies.

Mirlin Technologies also inform, as required, clients and other external parties of the company and industry-related issues that could affect their services and what steps the company is taking to reduce or avoid the impact on their operations. The organization's security commitments regarding the Mirlin Connect Services System are included in the services agreement.

MONITORING CONTROLS

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Mirlin Technologies' management performs monitoring activities to continuously assess the quality of internal control over time. Necessary corrective actions are taken as required to correct deviations from company policies and procedures. Employee activity and adherence to company policies and procedures are also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

Ongoing monitoring

Mirlin Technologies' management conducts quality assurance monitoring on a regular basis and additional training is provided based upon the results of monitoring procedures. Monitoring activities are used to initiate corrective action through department meetings, internal conference calls, and informal notifications.

Management's close involvement in Mirlin Technologies' operations helps to identify significant variances from expectations regarding internal controls. Upper management evaluates the facts and circumstances related to any suspected control breakdown. A decision to address any control's weakness is made based on whether the incident was isolated or requires a change in the company's procedures or personnel. The goal of this process is to ensure legal compliance and to maximize the performance of Mirlin Technologies' personnel.

Reporting deficiencies

Mirlin Technologies' internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

Monitoring of the Subservice Organization

Mirlin Technologies uses a subservice organization to provide hosting services.

Management of Mirlin Technologies receives and reviews the SOC 2 report of Azure on an annual basis. In addition, through its daily operational activities, the management of Mirlin Technologies monitors the services performed by Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

CHANGES TO THE SYSTEM DURING THE PERIOD

No significant changes have occurred to the services provided to user entities during the examination period.

SYSTEM INCIDENTS DURING THE PERIOD

No significant incidents have occurred to the service provided to user entities during the examination period.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Mirlin Technologies' controls related to the System cover only a portion of overall internal control for each user entity of Mirlin Technologies. It is not feasible for the trust services criteria related to the System to be achieved solely by Mirlin Technologies. Therefore, each user entity's internal controls should be evaluated in conjunction with Mirlin Technologies' controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Azure is responsible for maintaining physical security and environmental protection controls over the data centers hosting the Mirlin Technologies infrastructure.	CC6.4
2	Azure is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Mirlin Technologies' controls related to the Mirlin Connect Services System only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust service criteria related to the system to be achieved solely by Mirlin Technologies control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Mirlin Technologies.

User auditors should determine whether the following controls have been in place in operation at the user organization:

1. User entities should have controls in place to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
2. User entities are responsible for reporting issues with Mirlin Technologies systems and platforms.
3. User entities are responsible for understanding and complying with their contractual obligations to Mirlin Technologies.
4. User entities are responsible for notifying Mirlin Technologies of changes made to the administrative contact information.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, RELATED CONTROLS, AND TESTS OF CONTROLS

Trust Services Category, Criteria, Related Controls, and Tests of Controls

This SOC 2 Type 2 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design and operating effectiveness of controls to meet the criteria for the Security category 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* throughout the period July 1, 2024 to September 30, 2024.

The applicable trust services criteria and related controls specified by Mirlin Technologies are presented in Section 4 of this report.

Test procedures performed in connection with determining the operating effectiveness of controls detailed here in Section 4 are described below:

- Inquiries – Inquiry of appropriate personnel and corroboration with management.
- Observation – Observation of the application, performance, or existence of the control.
- Inspection – Inspection of documents and reports indicating the performance of the control.
- Reperformance – Reperformance of the control.

Footnotes for Test Results When No Tests of Operating Effectiveness Were Performed

1. The circumstances that warranted the operation of the control did not occur during the examination period; therefore, no tests of operating effectiveness were performed.
2. The operation of the control was performed outside the examination period; therefore, no tests of operating effectiveness were performed.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.1.2	The company requires employees to acknowledge the Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
		Inspected the Code of Conduct acknowledgments for a sample of active employees during the examination period to determine that the Code of Conduct was acknowledged at least annually.	No exceptions noted.
CC1.1.3	The company requires employees to review and acknowledge the information security policies at the time of hire and active employees to acknowledge the information security policies at least annually.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
		Inspected the information security policies acknowledgment for a sample of active employees to determine that the information security policies were acknowledged at least annually.	No exceptions noted.
CC1.1.4	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		performance evaluations for direct reports annually.	
CC1.1.5	The company performs background checks on new employees.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
CC1.1.6	Employees are required to review and acknowledge the confidentiality agreement at the time of hire.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
Criteria: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
The company does not have any independent board of directors; therefore, this criterion is not applicable.			
Criteria: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3.1	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the company's organizational chart to determine that the company maintained an organizational chart that described the organizational structure and reporting lines.	No exceptions noted.
CC1.3.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.3.3	The company requires employees to review and acknowledge the information security policies at the time of hire and active	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	employees to acknowledge the information security policies at least annually.	Inspected the information security policies acknowledgment for a sample of active employees to determine that the information security policies were acknowledged at least annually.	No exceptions noted.
Criteria: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4.1	The company performs background checks on new employees.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
CC1.4.2	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC1.4.4	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.
Criteria: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed. Sanction policies are documented within the information security policies and procedures.	Inspected the company's Code of Conduct to determine that the company had an approved Code of Conduct that is reviewed annually and updated as needed.	No exceptions noted.
		Inspected the company's information security policies and procedures to determine that sanction policies were documented within the information security policies and procedures.	No exceptions noted.
CC1.5.2	The company requires employees to acknowledge the Code of Conduct at the time of hire and active employees to acknowledge the Code of Conduct at least annually.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
		Inspected the Code of Conduct acknowledgments for a sample of active employees during the examination period to determine that the Code of Conduct was acknowledged at least annually.	No exceptions noted.
CC1.5.3	The company's managers are required to complete performance evaluations for direct reports at least annually.	Inspected the completed performance evaluation for a sample of employees to determine that the company's managers were required to complete performance evaluations for direct reports annually.	No exceptions noted.
CC1.5.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation,	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ENVIRONMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	security controls are formally assigned in the Information Security Policy.	operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	
CC1.5.5	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of the Information Security Policy review documentation, the Information Security Policies were reviewed and approved last June 2024. As the operation of the control was performed outside the examination period, therefore, no testing was performed.	No testing performed[2].
CC2.1.2	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC2.1.3	The company utilizes a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	Inspected the log management configurations to determine that the company utilized a log management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	No exceptions noted.
Criteria: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
INFORMATION AND COMMUNICATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC2.2.3	The company requires new employees to complete security awareness training at the time of hire and active employees to complete security training at least annually.	Inspected the security awareness training topics to determine that the security awareness training covered areas to educate personnel on information security topics and the latest trends to protect sensitive data.	No exceptions noted.
		Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
		Inspected the training records for a sample of active employees to determine that the company required employees to complete security awareness training annually.	No exceptions noted.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of the Information Security Policy review documentation, the Information Security Policies were reviewed and approved last June 2024. As the operation of the control was performed outside the examination period, therefore, no testing was performed.	No testing performed[2].
CC2.2.5	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company provided a description of its products and services to internal and external users.	No exceptions noted.
CC2.2.6	The company communicates system changes to authorized internal users.	Inspected the internal communication channel to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
Criteria: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3.1	The company's security commitments are communicated to customers in the Privacy Policy and Terms of Use.	Inspected the Privacy Policy and Terms of Use to determine that the company's security	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

INFORMATION AND COMMUNICATION

Control Number	Controls	Detailed Test of Controls	Test Results
		commitments were communicated to customers in the Privacy Policy and Terms of Use.	
CC2.3.2	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's Blog page to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3.3	The company describes its products and services to internal and external users.	Inspected the company's website to determine that the company described its products and services to internal and external users.	No exceptions noted.
CC2.3.4	The company has contact information on its website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website to determine that the company had a contact page on their website to allow users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3.5	The company has written agreements in place with vendors. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC2.3.6	The company notifies customers of critical system changes that may affect their processing.	Inspected the company's release notes to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1.2	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that 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.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
Criteria: COSO Principle 7: 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.			
CC3.2.1	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
		the identified threats, and mitigation strategies for those risks.	
CC3.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and subservice organizations was performed annually.	No exceptions noted.
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.2.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR business continuity/disaster recovery Plan to determine that the company has a documented business continuity/disaster recovery plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.
Criteria: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3.1	The company's risk assessments are performed at least annually. As part of this	Inspected the annual security risk assessment to determine that the company performed a risk	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	process, threats and changes (environmental, regulatory, and technological) 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.	assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	
CC3.3.2	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that 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.
Criteria: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4.1	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC3.4.2	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks	Inspected the company's Risk Assessment Policy to determine that the company had a documented risk management program in place that included guidance on the identification of potential threats, rating the significance of the risks associated with	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK ASSESSMENT			
Control Number	Controls	Detailed Test of Controls	Test Results
	associated with the identified threats, and mitigation strategies for those risks.	the identified threats, and mitigation strategies for those risks.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.1.2	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, there were no critical and high vulnerabilities identified in the penetration test; therefore, no testing was performed.	No testing performed[1].
CC4.1.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Per inquiry with management and inspection of the vulnerability scan report, there were no critical and high vulnerabilities identified in the vulnerability scans; therefore, no testing was performed.	No testing performed[1].
CC4.1.4	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and subservice organizations was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
MONITORING ACTIVITIES			
Control Number	Controls	Detailed Test of Controls	Test Results
Criteria: COSO Principle 17: 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.			
CC4.2.1	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively.	Inspected the company's compliance platform to determine that control self-assessments were performed annually, and corrective actions were taken based on relevant findings.	No exceptions noted.
CC4.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and subservice organizations was performed annually.	No exceptions noted.
CC4.2.3	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, there were no critical and high vulnerabilities identified in the penetration test; therefore, no testing was performed.	No testing performed[1].
CC4.2.4	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Per inquiry with management and inspection of the vulnerability scan report, there were no critical and high vulnerabilities identified in the vulnerability scans; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1.1	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that 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.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of the Information Security Policy review documentation, the Information Security Policies were reviewed and approved last June 2024. As the operation of the control was performed outside the examination period, therefore, no testing was performed.	No testing performed[2].
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC5.1.4	Role-based access is configured within Azure and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for Azure and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC5.2.2	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Secure Development and Change Management policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of the Information Security Policy review documentation, the Information Security Policies were reviewed and approved last June 2024. As the operation of the control was performed outside the examination period, therefore, no testing was performed.	No testing performed[2].
Criteria: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.	Per inquiry with management and inspection of the Information Security Policy review documentation, the Information Security Policies were reviewed and approved last June 2024. As the operation of the control was performed outside the examination period, therefore, no testing was performed.	No testing performed[2].

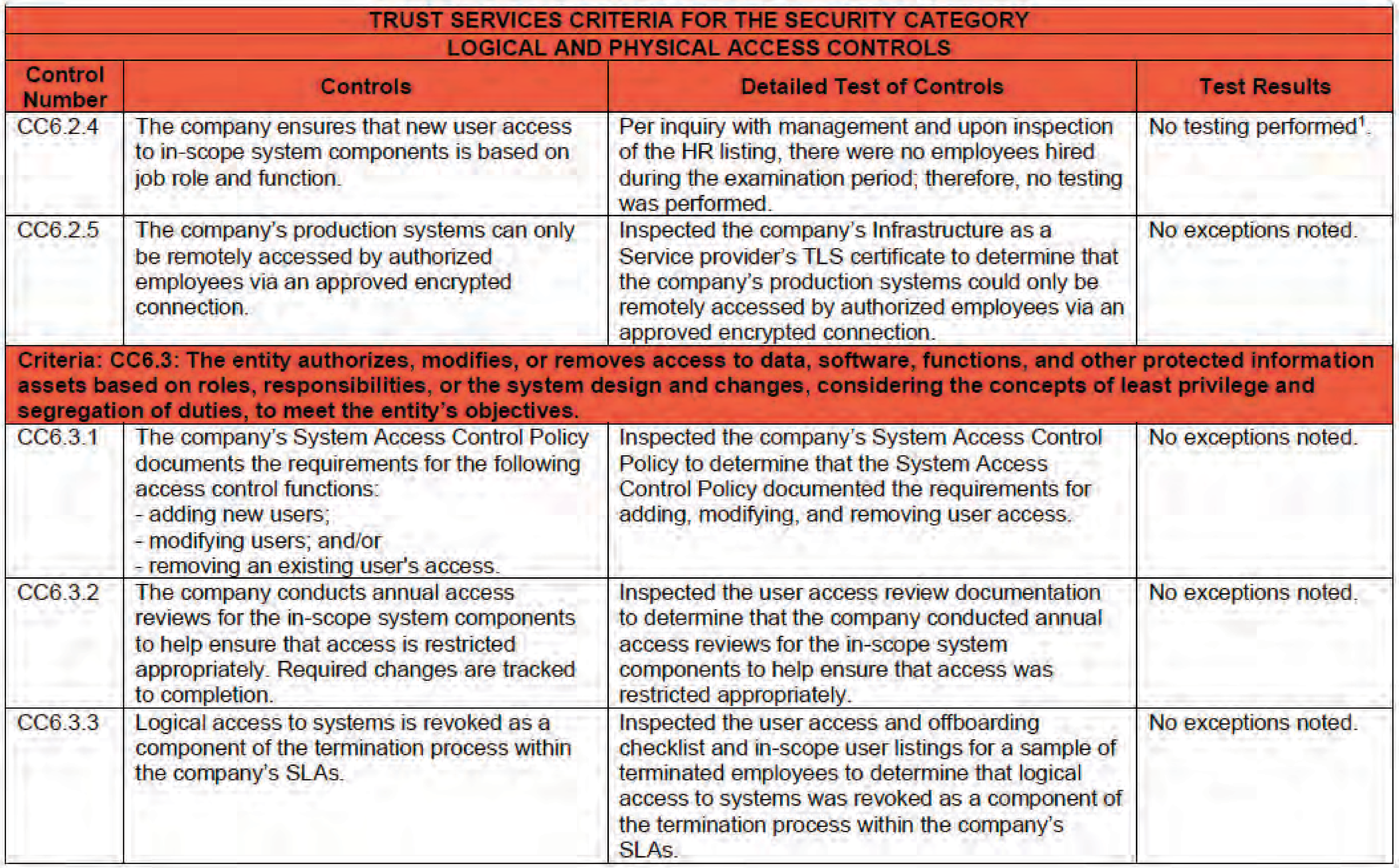
TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Secure Development and Change Management policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC5.3.3	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Secure Development and Change Management policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the annual security risk assessment to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CONTROL ACTIVITIES			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC5.3.6	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that 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.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Information Security Policy.	Inspected the company's Information Security Policy to determine roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in the Information Security Policy.	No exceptions noted.
CC5.3.8	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and - annual review of critical vendors and subservice organizations.	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.
		Inspected the vendor review to determine that a review of critical vendors and subservice organizations was performed annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC6.1: 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.			
CC6.1.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.1.2	The company has a Data Classification Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Inspected the company's Data Classification Policy to determine that the company had a Data Classification Policy in place to help ensure that confidential data was properly secured and restricted to authorized personnel.	No exceptions noted.
CC6.1.3	The company's databases housing sensitive customer data are encrypted at rest.	Inspected the encryption configurations to determine that the company databases housing sensitive customer data are encrypted at rest.	No exceptions noted.
CC6.1.4	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the company's Encryption Policy to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
		Inspected the list of users with privileged access to encryption keys to determine that the company restricted privileged access to authorized users with a business need.	No exceptions noted.
CC6.1.5	Role-based access is configured within Azure and other supporting applications to enforce the segregation of duties and restrict access to confidential information.	Inspected the system configuration for Azure and other supporting applications to determine that role-based access was configured to enforce segregation of duties and restrict access to confidential information.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.1.6	The company restricts privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	Inspected the list of users with privileged access to the cloud infrastructure and application to determine that the company restricted privileged access to the network, application, databases, and supporting cloud infrastructure to authorized users with a business need.	No exceptions noted.
CC6.1.7	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the list of users with privileged access to the firewall to determine that the company restricted privileged access to the firewall to authorized users with a business need.	No exceptions noted.
CC6.1.8	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.1.9	The company ensures that new user access to in-scope system components is based on job role and function.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
CC6.1.10	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the password configurations and written password policy to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.1.12	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
		remotely accessed by authorized employees via an approved encrypted connection.	
CC6.1.13	The company maintains a formal inventory of production system assets.	Inspected an inventory listing of information assets to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
CC6.1.14	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network configurations to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.
Criteria: 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.			
CC6.2.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.2.2	The company conducts annual access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted annual access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.



TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.2.4	The company ensures that new user access to in-scope system components is based on job role and function.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
CC6.2.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: CC6.3: 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, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives.			
CC6.3.1	The company's System Access Control Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Inspected the company's System Access Control Policy to determine that the System Access Control Policy documented the requirements for adding, modifying, and removing user access.	No exceptions noted.
CC6.3.2	The company conducts annual access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected the user access review documentation to determine that the company conducted annual access reviews for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the company's SLAs.	Inspected the user access and offboarding checklist and in-scope user listings for a sample of terminated employees to determine that logical access to systems was revoked as a component of the termination process within the company's SLAs.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC6.3.4	The company ensures that new user access to in-scope system components is based on job role and function.	Per inquiry with management and upon inspection of the HR listing, there were no employees hired during the examination period; therefore, no testing was performed.	No testing performed[1].
CC6.3.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
Criteria: CC6.4: 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.			
CC6.4.1	Management contracts with Azure to provide physical and logical access security of its production systems; therefore, this criterion is the responsibility of the subservice organization.	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	
Criteria: CC6.5: 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.			
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Inspected the data retention and disposal procedures to determine that the company had formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices.	Per inquiry with management and inspection of media and data disposal records, no disposals occurred during the examination period; therefore, no testing was performed.	No testing performed[1].
CC6.5.3	The destruction of physical assets hosting the production environment is the responsibility of	This control activity is the responsibility of the subservice organization. Refer to the Subservice Organization section above for controls managed by the subservice organization.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	Azure; therefore, part of this criterion is the responsibility of the Subservice Organization.		
Criteria: CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the company's Infrastructure as a Service provider's TLS certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid MFA method.	Inspected the MFA configurations to determine that the company's production systems could only be remotely accessed by authorized employees possessing a valid MFA method.	No exceptions noted.
CC6.6.3	The firewall is configured to prevent unauthorized access to the company's network.	Inspected the firewall rules to determine that the firewall was configured to prevent unauthorized access to the company's network.	No exceptions noted.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.6.5	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
Criteria: CC6.7: 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.			
CC6.7.1	The company encrypts portable devices when used.	Inspected the company's Encryption to determine that the company encrypted portable media devices when used.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	Controls	Detailed Test of Controls	Test Results
		Inspected the encryption configurations for a sample of devices to determine that the company encrypted portable media devices when used.	No exceptions noted.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the company's website and TLS certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	No exceptions noted.
CC6.7.3	The company has a mobile device management system in place to centrally manage mobile devices supporting the service.	Inspected the company's mobile device management system to determine that the company had a mobile device management system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
Criteria: CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks. The anti-malware software is configured to scan workstations daily and install updates as new updates/signatures are available.	Inspected the anti-malware configurations for a sample of workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks.	No exceptions noted.
		Inspected the anti-malware configurations to determine that the anti-malware software was configured to scan workstations daily and install updates as new updates/signatures were available.	No exceptions noted.
CC6.8.2	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and	Inspected the company's Secure Development and Change Management policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
LOGICAL AND PHYSICAL ACCESS CONTROLS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
	maintenance of information systems and related technology requirements.	changes), and maintenance of information systems and related technology requirements.	

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC7.1: 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.			
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Secure Development and Change Management policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1.3	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Per inquiry with management and inspection of the vulnerability scan report, there were no critical and	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY

SYSTEM OPERATIONS

Control Number	Controls	Detailed Test of Controls	Test Results
		high vulnerabilities identified in the vulnerability scans; therefore, no testing was performed.	
CC7.1.4	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, there were no critical and high vulnerabilities identified in the penetration test; therefore, no testing was performed.	No testing performed[1].
CC7.1.5	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's Change Management Policy to determine that the company had a configuration management procedure in place to ensure that system configurations were deployed consistently throughout the environment.	No exceptions noted.
CC7.1.6	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
Criteria: CC7.2: 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.			
CC7.2.1	The company uses an Intrusion Detection System (IDS) to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the IDS configurations to determine that the company used an IDS to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC7.2.2	The company utilizes a log management tool to identify events that may potentially impact	Inspected the log management tool configurations to determine that the company utilized a log	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
	the company's ability to achieve its security objectives.	management tool to identify events that may potentially impact the company's ability to achieve its security objectives.	
CC7.2.3	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the company's Vulnerability Management Policy to determine that the company's formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	No exceptions noted.
CC7.2.4	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Inspected the monitoring tool configurations to determine that an infrastructure monitoring tool was utilized to monitor systems, infrastructure, and performance and generated alerts when specific predefined thresholds were met.	No exceptions noted.
CC7.2.5	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Per inquiry with management and inspection of the vulnerability scan report, there were no critical and high vulnerabilities identified in the vulnerability scans; therefore, no testing was performed.	No testing performed[1].
CC7.2.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, there were no critical and high vulnerabilities identified in the penetration test; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC7.2.7	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.	Per inquiry with management and inspection of incident records, there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed[1].
Criteria: CC7.3: 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.			
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.3.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of incident records, there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed[1].
Criteria: 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.			
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.4.2	The company's security incidents are logged, tracked, resolved, and communicated to	Inspected the company's Incident Response Plan to determine that the company's security incidents	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
	affected or relevant parties by management according to the company's security incident response policy and procedures.	were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	
		Per inquiry with management and inspection of incident records, there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed[1].
CC7.4.3	The company has documented Incident Response Plan and tests it at least annually.	Inspected the company's Incident Response Plan to determine that the incident response plan was in place and approved by management.	No exceptions noted
		Inspected the company's incident response plan test notes to determine that the company tests its incident response plan at least annually.	No exceptions noted.
Criteria: CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.	Inspected the company's Incident Response Plan and the compliance platform to determine that the company had security incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.5.2	The company's security incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Inspected the company's Incident Response Plan to determine that the company's security incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	No exceptions noted.
		Per inquiry with management and inspection of incident records, there were no incidents reported during the examination period; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
SYSTEM OPERATIONS			
Control Number	Controls	Detailed Test of Controls	Test Results
CC7.5.3	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.5.4	The company has a documented business continuity/disaster recovery (BC/DR) Plan and tests it at least annually.	Inspected the company's BC/DR business continuity/disaster recovery Plan to determine that the company has a documented business continuity/disaster recovery plan.	No exceptions noted.
		Inspected the company's latest BC/DR Plan tabletop exercise meeting minutes to determine that the BC/DR plan was tested annually.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1.1	The company has a formal SDLC methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Inspected the company's Secure Development and Change Management policies to determine that the company had a formal SDLC methodology in place that governed the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	No exceptions noted.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	Inspected the company's Secure Development and Change Management policies to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
		Inspected the documentation for a sample of changes to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved before being implemented in the production environment.	No exceptions noted.
CC8.1.3	Segregation of duties is in place to prevent developers from pushing changes to production.	Inspected the user listing for the company's change management tool and branch protection rules to determine that developers do not have access to the production environment.	No exceptions noted.
CC8.1.4	The company restricts access to the production environment to authorized personnel.	Inspected the users with access to production to determine that the company restricts access to the production environment to authorized personnel.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
CHANGE MANAGEMENT			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
CC8.1.5	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC8.1.6	The company's penetration testing is performed at least annually. A remediation plan is developed, and changes are implemented to remediate critical and high vulnerabilities in accordance with SLAs.	Inspected the completed penetration report to determine that a penetration test was performed annually.	No exceptions noted.
		Per inquiry with management and inspection of the penetration test report, there were no critical and high vulnerabilities identified in the penetration test; therefore, no testing was performed.	No testing performed[1].
CC8.1.7	Vulnerability scans are performed quarterly on in-scope systems. Critical and high vulnerabilities are tracked to remediation in accordance with SLAs.	Inspected the completed vulnerability scan reported to determine that vulnerability scans were performed quarterly on in-scope systems.	No exceptions noted.
		Per inquiry with management and inspection of the vulnerability scan report, there were no critical and high vulnerabilities identified in the vulnerability scans; therefore, no testing was performed.	No testing performed[1].

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	**Controls**	**Detailed Test of Controls**	**Test Results**
Criteria: CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) 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 annual security risk assessment to determine that the company performed a risk assessment annually that included the identification and assessment of threats and changes to services commitments, a consideration of the potential for fraud, and how fraud may impact the achievement of objectives.	No exceptions noted.
CC9.1.2	The company has a documented risk management program in place that 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 company's Risk Assessment Policy to determine that the company had a documented risk management program in place that 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.
Criteria: CC9.2: The entity assesses and manages risks associated with vendors and business partners.			
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include security and confidentiality commitments applicable to that entity.	Inspected the Terms of Service for vendors and related third parties to determine that security and confidentiality commitments were in place for vendors and related third parties.	No exceptions noted.
CC9.2.2	The company has a third-party management program in place. Components of this program include: - critical vendor inventory. - vendor's security requirements; and	Inspected the company's Vendor Management Policy to determine that the company had a third-party management program in place that included the security requirements for vendors.	No exceptions noted.
		Inspected the vendor listing to determine that the critical vendor inventory was in place.	No exceptions noted.

TRUST SERVICES CRITERIA FOR THE SECURITY CATEGORY			
RISK MITIGATION			
Control Number	Controls	Detailed Test of Controls	Test Results
	- annual review of critical vendors and subservice organizations.	Inspected the vendor review to determine that a review of critical vendors and subservice organizations was performed annually.	No exceptions noted.