SOC 2 Report

for

Windsor Group AG

A Type 2 Independent Service Auditor's Report on Controls Relevant to Security

February 20, 2026 to May 20, 2026

Audit & Attestation By:

PRESCIENT
ASSURANCE

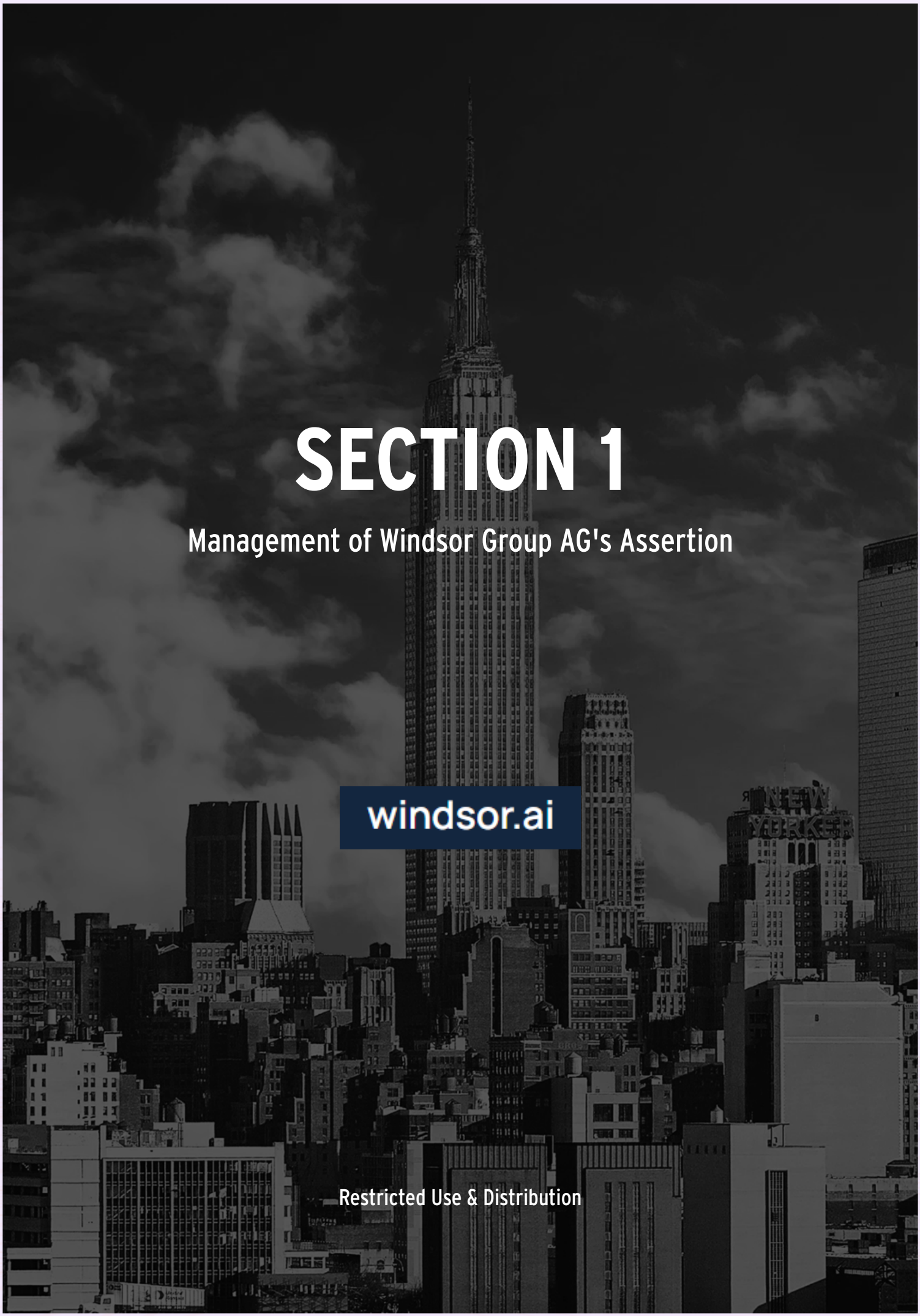
Restricted Use & Distribution

Prescient Assurance LLC.
1900 Church Street, Suite 300
Nashville, TN, 37203

CPA

www.prescientassurance.com
info@prescientassurance.com
+1 646 209 7319

Table of Contents



SECTION 1

Management of Windsor Group AG's Assertion

windsor.ai

Restricted Use & Distribution

Management of Windsor Group AG's Assertion

We have prepared the accompanying description of Windsor Group AG's (“Windsor Group AG”) windsor.ai system titled “Description of Windsor Group AG's system” throughout the period February 20, 2026, to May 20, 2026, 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, in AICPA Description Criteria (With Revised Implementation Guidance—2022) (2018 description criteria). The description is intended to provide report users with information about the Windsor Group AG’s system that may be useful when assessing the risks arising from interactions with the Windsor Group AG’s system, particularly information about system controls that Windsor Group AG 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" set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria (With Revised Points of Focus - 2022) (2017 applicable trust services criteria).

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

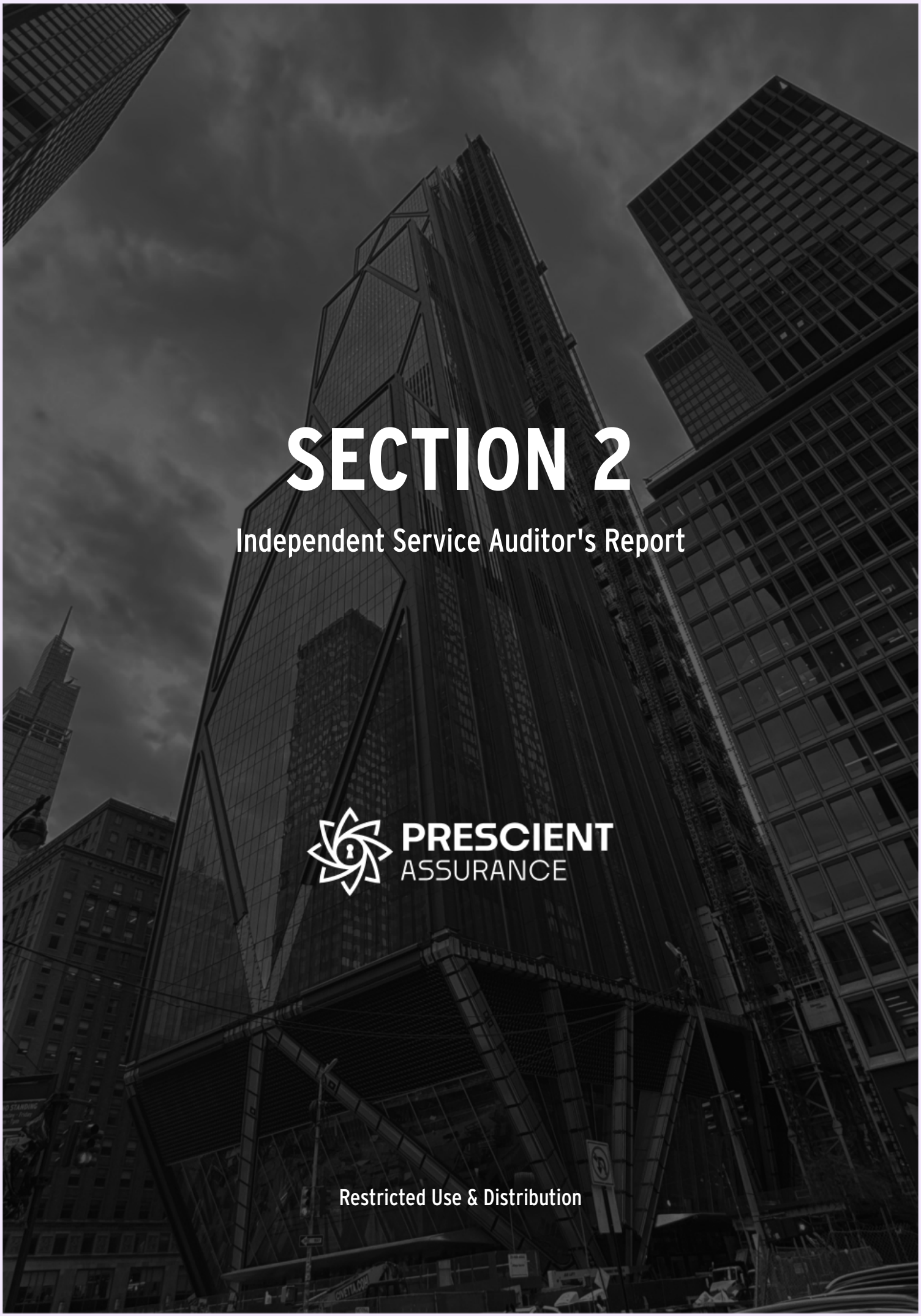
The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Windsor Group AG, to achieve Windsor Group AG’s service commitments and system requirements based on the applicable trust services criteria. The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

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

1. The description presents windsor.ai system that was designed and implemented throughout the period February 20, 2026, to May 20, 2026, in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period February 20, 2026, to May 20, 2026, to provide reasonable assurance that Windsor Group AG's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Windsor Group AG's controls throughout that period.
3. The controls stated in the description operated effectively throughout the period February 20, 2026, to May 20, 2026, to provide reasonable assurance that Windsor Group AG's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of Windsor Group AG's controls operated effectively throughout that period.

Niklas Kolster

Niklas Kolster
CEO
Windsor Group AG



SECTION 2

Independent Service Auditor's Report

PRESCIENT ASSURANCE

Restricted Use & Distribution

Independent Service Auditor's Report

To: Management of Windsor Group AG

Scope

We have examined Windsor Group AG's ("Windsor Group AG") accompanying description of its windsor.ai system found in Section 3, titled "Description of Windsor Group AG's system" throughout the period February 20, 2026, to May 20, 2026, 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, in AICPA Description Criteria (With Revised Implementation Guidance—2022) (2018 description criteria), and the suitability of the design and operating effectiveness of controls stated in the description throughout the period February 20, 2026, to May 20, 2026, to provide reasonable assurance that Windsor Group AG's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security" set forth in TSP section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy, in AICPA Trust Services Criteria (With Revised Points of Focus - 2022) (2017 applicable trust services criteria).

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

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

Service Organization's Responsibilities

Windsor Group AG is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the system to provide reasonable assurance that Windsor Group AG's service commitments and system requirements were achieved. In Section 1, Windsor Group AG has provided the accompanying assertion titled "Management of Windsor Group AG's Assertion" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Windsor Group AG is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the AICPA. 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 to meet our other ethical responsibilities in accordance with relevant ethical requirements relating to the engagement.

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

1. Obtaining an understanding of the system and the service organization's service commitments and system requirements
2. 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
3. Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
4. 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
5. 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
6. 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 users may consider important to meet their informational needs. There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

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

Other Matters

We do not express an opinion on Section 5 – Other Information.

Opinion

In our opinion, in all material respects,

1. The description presents windsor.ai system that was designed and implemented throughout the period February 20, 2026, to May 20, 2026, in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period February 20, 2026, to May 20, 2026, to provide reasonable assurance that Windsor Group AG's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Windsor Group AG's controls throughout that period.
3. The controls stated in the description operated effectively throughout the period February 20, 2026, to May 20, 2026, to provide reasonable assurance that Windsor Group AG's 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 Windsor Group AG's controls operated effectively throughout that period.

Restricted Use

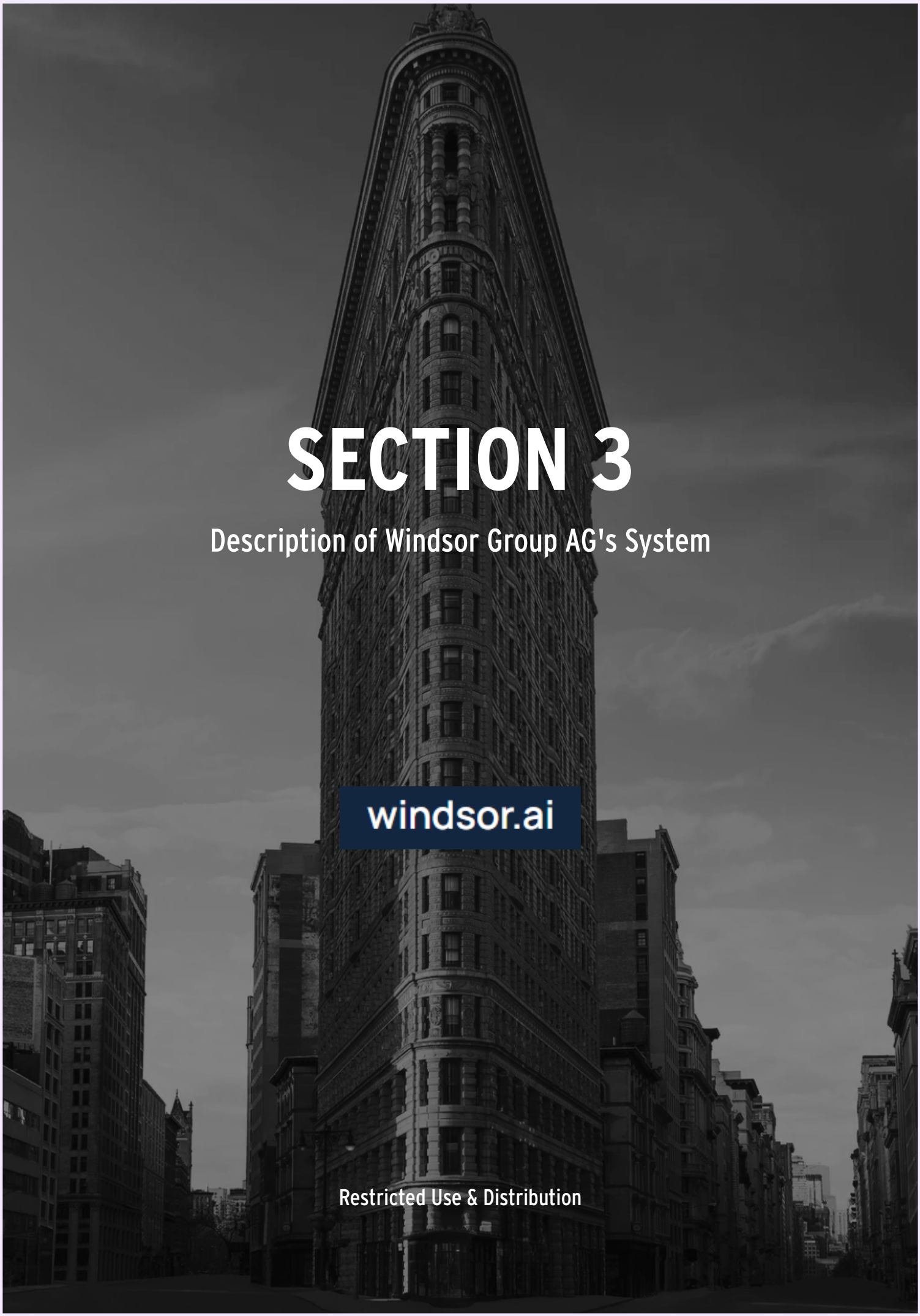
This report, including the description of tests of controls and results thereof in Section 4, is intended solely for the information and use of Windsor Group AG, user entities of Windsor Group AG's system during some or all of the period February 20, 2026, to May 20, 2026, business partners of Windsor Group AG subject to risks arising from interactions with the 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:

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

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

Prescient Assurance

Prescient Assurance LLC
Nashville, TN
July 29, 2026



SECTION 3

Description of Windsor Group AG's System

windsor.ai

Restricted Use & Distribution

DC 1: Company Overview and Types of Products and Services Provided

Company Background

Windsor Group AG is a software as a service company headquartered in Zug Switzerland. The company automates marketing data pipelines and reporting for businesses.

Description of services provided

Windsor.ai has built connectors to more than 50 different online platforms. The platform makes it easy to pull in all marketing data from all of these platforms and create reports on the marketing performance for businesses. Windsor.ai optimizer proposes optimizations to the marketing channel budget allocation.

Windsor.ai provides the connections to marketing data platforms and data pipelines; automating marketing reporting, multitouch attribution, and marketing budget optimization recommendations.

DC 2: The Principal Service Commitments and System Requirements

Windsor Group AG designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that Windsor Group AG makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Windsor Group AG has established for the services. The system services are subject to the Security commitments established internally for its services.

Windsor.ai service commitments are communicated SLA's or in the Master agreements or in the online description of the services.

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

- System features and configuration settings designed to authorize user access while restricting unauthorized users from accessing information not needed for their role
- Use of intrusion detection systems to prevent and identify potential security attacks from users outside the boundaries of the system
- Quarterly vulnerability scans over the system and network, and annual penetration tests over the production environment
- Operational procedures for managing security incidents and breaches, including notification procedures
- Use of encryption technologies to protect customer data both at rest and in transit
- Use of data retention and data disposal.

DC 3: The Components of the System Used to Provide the Services

The system 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 uses 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 are mobile applications or desktop or laptop applications.

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.

3.1 Primary Infrastructure

Windsor Group AG maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, inventory type, description and owner.

Infrastructure	Service	Purpose
Hetzner Online GmbH	Cloud provider	Provides cloud hosting and infrastructure services for production systems and applications.

3.2 Primary Software

Windsor Group AG is responsible for managing the development and operation of the windsor.ai system including infrastructure components such as servers, databases, and storage systems. The in-scope Windsor Group AG software components are shown in the table provided below:

System/Application	Service provided	Purpose
Cloudflare	Network Security	Provides DNS management, content delivery network (CDN) services, web traffic protection, and performance optimization.
GitLab	Version Control	Source code repository and DevOps platform used for version control, code review, and CI/CD pipeline management.
Google Workspace	Productivity / Identity Management	Provides email, collaboration, document management, and identity management services for employees.
Trello	Project Management	Task and project management platform used to track workflows, assignments, and team collaboration.
JIRA	Project Management	Organize work into projects, epics, task, and subtasks. Issue Tracking tool
Slack	Communication	Collaboration Platform for internal communication
Discord	Communication	Communication tool for internal communication

3.3 People

Windsor Group AG employs dedicated team members to handle major product functions, including operations, and support. The IT/Engineering Team monitors the environment, as well as manages data backups and recovery.

Windsor Group AG has a staff of approximately 33 organized in the following functional areas:

Management: Individuals who are responsible for enabling other employees to perform their jobs effectively and for maintaining security and compliance across the environment. This includes:

- Founder & CEO - Niklas Kolster
- CTO - Octavian Corlade
- COO - Matthias Kraaz

Operations: Responsible for maintaining the availability of production infrastructure and managing access and security for production infrastructure. Only members of the Operations team have access to the production environment. Members of the Operations team may also be members of the Engineering team.

Information Technology: Responsible for managing laptops, software, and other technology involved in employee productivity and business operations.

Product Development: Responsible for the development, testing, deployment, and maintenance of the source code for the system. Responsible for the product life cycle, including adding additional product functionality.

3.4 Data

Data as defined by Windsor Group AG, constitutes the following:

User and account data - this includes Personally Identifiable Information (PII) and other data from employees, customers, users (customers' employees), and other third parties such as suppliers, vendors, business partners, and contractors. This collection is permitted under the Terms of Service and Privacy Policy (as well as other separate agreements with vendors, partners, suppliers, and other relevant third parties). Access to PII is controlled through processes for provisioning system permissions, as well as ongoing monitoring activities, to ensure that sensitive data is restricted to employees based on job function.

Data is categorized in the following major types of data used by Windsor Group AG:

Category	Description	Examples
Company data	Information collected and used by Windsor Group AG to operate the business. Windsor Group AG upholds the highest level of security and restricted availability for this information.	• Legal documents • Contractual agreements • Employee PII • Employee salaries
Internal	Internal information whose access is approved by management and that is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences
Customer data	Information received from customers for processing or storage by Windsor Group AG. Windsor Group AG upholds the highest level of security and restricted availability for this information.	• Customer operating data • Customer PII • Customers' clients' PII • Anything subject to a confidentiality agreement with a customer
Public	Non-confidential information that can be made public without any likely adverse or significant implications for Windsor Group AG.	• Press releases • Public website

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, if any. Customer data is captured which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Windsor Group AG has policies and procedures in place to ensure proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.5 Processes and Procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications

3.5.1 Physical Security

Windsor Group AG's production servers are maintained by Hetzner Online GmbH. The physical and environmental security protections are the responsibility of Hetzner Online GmbH. Windsor Group AG reviews the attestation reports and performs a risk analysis of Hetzner Online GmbH on at least an annual basis.

3.5.2 Logical Access

Windsor Group AG provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

Access to these systems is split into admin roles, user roles, and no access roles. User access and roles are reviewed on a quarterly basis to ensure least privilege access.

Management is responsible for provision of access to the system based on the employee's role and performing a background/reference check. The employee is responsible for reviewing Windsor Group AG's policies and completing security training at the time of hire and annually thereafter.

When an employee is terminated, management is responsible for deprovisioning access to all in scope systems within 24 business hours of the employee's termination.

3.5.3 Computer Operations - Backups

Customer data is backed up and monitored by the product for completion and exceptions. If there is an exception, product will perform troubleshooting to identify the root cause and either rerun the backup or run the backup as part of the next scheduled backup job.

Backup infrastructure is maintained in Hetzner Online GmbH with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer Operations - Availability

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

Windsor Group AG internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Windsor Group AG utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open-source dependencies and maintains an internal SLA for responding to those issues.

3.5.5 Change Management

Windsor Group AG maintains documented Systems Development Life Cycle (SDLC) policies and procedures to guide personnel in documenting and implementing application and infrastructure changes. Change control procedures include change request and initiation processes, documentation requirements, development practices, quality assurance testing requirements, and required approval procedures.

A ticketing system, JIRA, is utilized to document the change control procedures for changes in the application and implementation of new changes. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

Version control software, GitLab, is utilized to maintain source code versions and migrate source code through the development process to the production environment. The version control software maintains a history of code changes to support rollback capabilities and tracks changes to developers.

3.5.6 Data Communications

Windsor Group AG has elected to use a platform-as-a-service (PaaS), Hetzner Online GmbH, to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS, Hetzner Online GmbH, simplifies Windsor Group AG's logical network configuration by providing an effective firewall around all the Windsor Group AG 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.

3.6 Boundaries of the System

The boundaries of the windsor.ai system are the specific aspects of the Windsor Group AG's 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 windsor.ai system.

This report does not include the Cloud Hosting Services provided by Hetzner Online GmbH at multiple facilities.

DC 4: Disclosures About Identified Security Incidents

A. Incidents Pertaining to the Audit Period

No significant security incidents have occurred during the audit period that would have a material effect on the suitability of the design and operating effectiveness of the controls and/or description of the system covered in Section 3 of this report.

B. Incidents Subsequent to the Audit Period

Management is not aware of any incidents that occurred subsequent to the period covered by Section 3 of this report through the date of the service auditor’s report that would have a significant effect on management’s assertion and description of its system.

DC 5: The Applicable Trust Services Criteria and the Related Controls Designed to Provide Reasonable Assurance that the Service Organization’s Service Commitments and System Requirements were Achieved

5.1 Integrity and Ethical Values

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

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

- The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.
- The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.
- The company requires employees to sign a confidentiality agreement during onboarding.

- The company requires contractors to sign a confidentiality agreement at the time of engagement.
- The company performs reference checks on new employees.

5.2 Commitment to Competence

Windsor Group AG's management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

- The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
- Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.
- The company managers are required to complete performance evaluations for direct reports at least annually.

5.3 Management's Philosophy and Operating Style

The management team meets frequently to be briefed on technology changes that impact the way Windsor Group AG can help customers build data workflows, as well as new security technologies that can help protect those workflows, and finally any regulatory changes that may require Windsor Group AG to alter its software to maintain legal compliance. Major planned changes to the business are also reviewed by the management team to ensure they can be conducted in a way that is compatible with Windsor Group AG's core product offerings and duties to new and existing customers.

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

- The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.
- The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.
- The company's board of directors meets at least annually and maintains formal meeting minutes.

5.4 Organizational Structure and Assignment of Authority and Responsibility

Windsor Group AG's 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.

Windsor Group AG's assignment of authority and responsibility activities include 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:

- The company maintains an organizational chart that describes the organizational structure and reporting lines.
- Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.

5.5 HR Policies and Practices

Windsor Group AG's 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:

- The company requires employees to sign a confidentiality agreement during onboarding.
- The company requires contractors to sign a confidentiality agreement at the time of engagement.
- The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.
- The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.

5.6 Risk Assessment Process

Windsor Group AG’s risk assessment process identifies and manages risks that could potentially affect Windsor Group AG’s ability to provide reliable and secure services to customers. As part of this process, Windsor Group AG 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 reevaluated annually, and tasks are incorporated into the regular Windsor Group AG product development process so they can be dealt with predictably and iteratively.

5.6.1 Integration with Risk Assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of Windsor Group AG’s system; as well as the nature of the components of the system result in risks that the criteria will not be met. Windsor Group AG addresses these risks through the implementation of suitably 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, Windsor Group AG’s management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.7 Information and Communication Systems

Information and communication are an integral component of Windsor Group AG’s 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.

Windsor Group AG uses several information and communication channels, such as Slack and Discord, internally to share information with management, employees, contractors, and customers. Windsor Group AG uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools such as Trello and Google Workspace. Finally, Windsor Group AG uses in-person and video “all hands” meetings to communicate company priorities and goals from management to all employees.

5.8 Monitoring Controls

Management monitors security related internal controls to ensure that they are operating as intended and that controls are modified as conditions change. Windsor Group AG's 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 is also monitored. This process is accomplished through ongoing monitoring activities, separate evaluations, or a combination of the two.

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

- The company's formal policies outline the requirements for the following functions related to IT, Engineering, vulnerability management, and system monitoring.

5.8.1 Ongoing Monitoring

Windsor Group AG's management conducts quality assurance monitoring on a regular basis and additional training is provided based upon 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 Windsor Group AG's 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 for addressing 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 Windsor Group AG's personnel.

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

- The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.
- The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.

5.8.2 Separate Evaluations

Management performs separate evaluations of the organization's internal control environment on a periodic basis to determine whether controls are appropriately designed and operating effectively. These evaluations are conducted independently of routine operational monitoring and may occur periodically or following significant organizational, technological, or regulatory changes. Results are documented, reviewed by management, and used to identify opportunities for improvement.

5.9 Reporting Deficiencies

Windsor Group AG's 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.

DC 6: Complementary User Entity Controls (CUECs)

Windsor Group AG's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls.

It is not feasible for all the Trust Services Criteria related to Windsor Group AG's services to be solely achieved by Windsor Group AG's control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Windsor Group AG.

The following complementary user entity controls should be implemented by user entities to provide

additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

Criteria	User Entity Responsibilities
CC2.1	User entities have policies and procedures that require reporting any material changes to their control environment that may adversely affect the ability of Windsor Group AG to deliver service.
CC2.1	User entities have controls that require providing notice to Windsor Group AG of any material changes in security requirements and the authorized users list.
CC2.3	User entities have policies and procedures to determine how to file inquiries, complaints, or disputes to Windsor Group AG.
CC6.1	User entities have policies and procedures that grant Windsor Group AG system access only to authorized and trained personnel.
CC6.4	User entities deploy physical security and environmental controls for all local and remote devices and access points that access the Windsor Group AG system.
CC6.6	User entities have policies and procedures for controlling user IDs and passwords that are used to access the Windsor Group AG system.

DC 7: Complementary Subservice Organization Controls (CSOCs)

The description does not extend to the services provided by Hetzner Online GmbH (the subservice organization). Section 4 of this report and the description of the system only cover the relevant trust services criteria and related controls in support of the achievement of Windsor Group AG's service commitments and system requirements and exclude the related controls of the subservice organization.

Although the subservice organization has been carved out for the purposes of this report, Windsor Group AG's management has assumed, in the design of the system, that certain complementary subservice organization controls (CSOCs) would be implemented by the subservice organization. Such controls are necessary, in combination with controls at Windsor Group AG, to provide reasonable assurance that Windsor Group AG's service commitments and system requirements were achieved. Because the related service commitments and system requirements can only be achieved if the CSOCs are suitably designed and operating effectively during the period February 20, 2026, to May 20, 2026, each user entity must evaluate Windsor Group AG's controls, related tests of controls, and results of tests described in section 4 of this report, considering the types of related CSOCs expected to be implemented at the subservice organization as shown below.

Subservice Organization	Services Provided	Criteria	Expected CSOCs
Hetzner Online GmbH	Infrastructure Hosting	CC6.4	Physical access to data centers is approved by an authorized individual.
			Physical access rights are revoked in a timely manner when no longer required.
			Physical access to data centers is reviewed periodically by appropriate personnel.
			Data center facilities are monitored using physical security monitoring controls, including video surveillance.
			Access to server locations is managed by electronic access control devices.
		CC7.2	Electronic intrusion detection systems are installed

			within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.
		CC7.5	Backup and recovery capabilities are maintained to support restoration of systems following security incidents or system failures.

Management of Windsor Group AG receives and reviews independent third-party assessment reports of its subservice organization annually. In addition, Windsor Group AG management monitors the services performed by the subservice organization to determine whether operations and controls expected to be implemented at the subservice organization are suitably designed and operating effectively.

DC 8: Any Specific Criterion of the Applicable Trust Services Criteria that is Not Relevant to the System and the Reasons it is Not Relevant

There were no specific Security Trust Services Criteria as set forth in TSP Section 100 that were not relevant to the windsor.ai system as presented in this report.

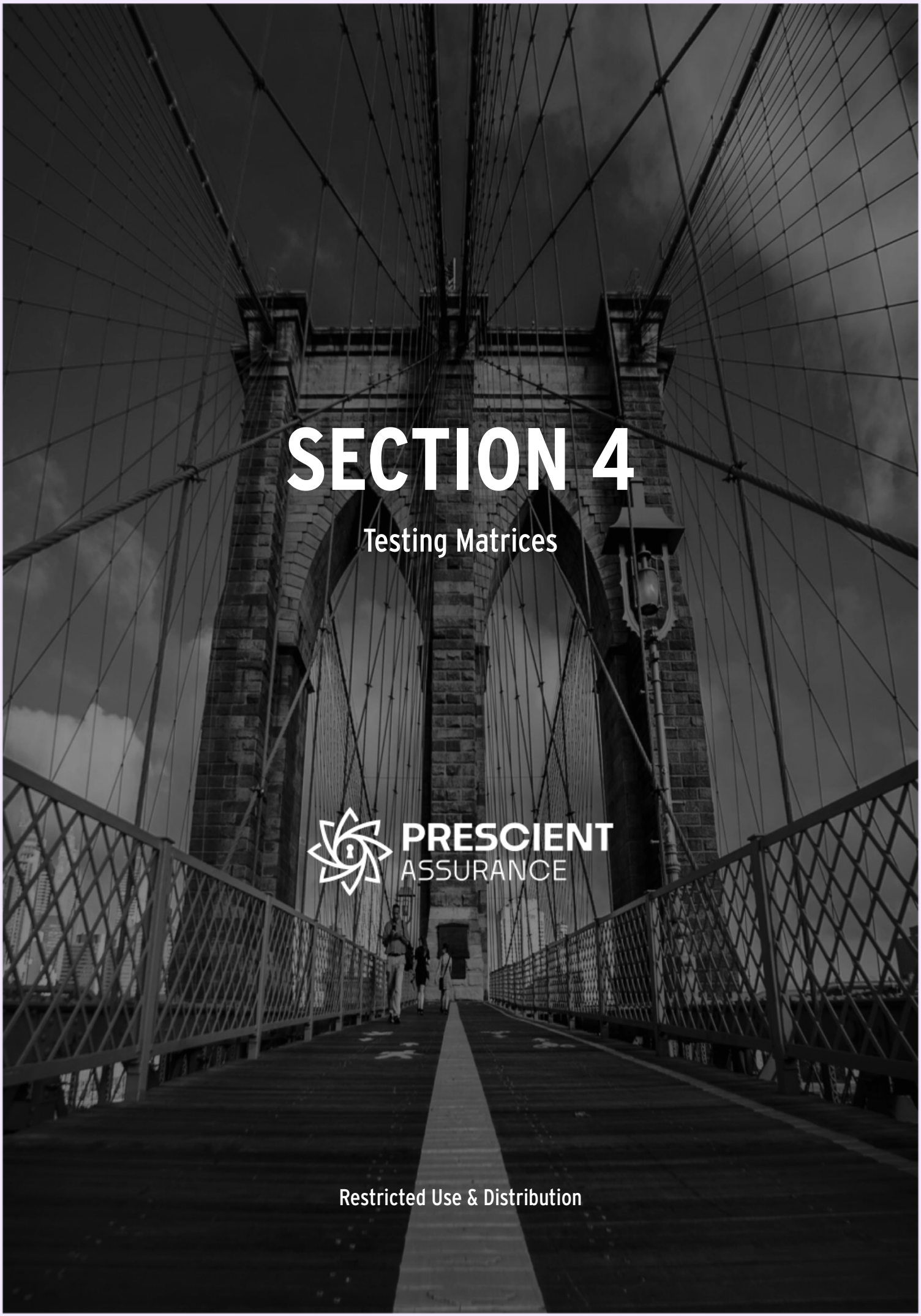
DC 9: Disclosures of Significant Changes

A. Significant Changes and Events during the Audit Period

No significant changes and events have occurred during the audit period that would have a material effect on the suitability of the design and operating effectiveness of the controls and/or description of the system covered in Section 3 of this report.

B. Significant Changes and Events subsequent to the Audit Period

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



SECTION 4

Testing Matrices

PRESCIENT ASSURANCE

Restricted Use & Distribution

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to the windsor.ai system provided by Windsor Group AG. The scope of the testing was restricted to the windsor.ai system, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period February 20, 2026, to May 20, 2026.

Tests of Operating Effectiveness

The tests applied to test the Operating Effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance, that all applicable trust services criteria were achieved during the period. In selecting the tests of controls, Prescient Assurance LLC considered various factors including, but not limited to, the following:

- The nature of the control and the frequency with which it operates;
- The control risk mitigated by the control;
- The effectiveness of entity-level controls, especially controls that monitor other controls;
- The degree to which the control relies on the effectiveness of other controls; and
- Whether the control is manually performed or automated.

Using the work of an Internal Audit Function

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

Types of Tests Generally Performed

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

Test Types	Description of Tests
Inquiry	Inquired of relevant personnel with the requisite knowledge and experience regarding the performance and application of the related control activity. This included in-person interviews, telephone calls, e-mails, web-based conferences, or a combination of the preceding.
Inspection	Inspected documents and records indicating performance of the control. This includes, but is not limited to, the following: • Inspection of source documentation and authorizations to verify transactions processed. • Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Inspection of systems documentation, configurations, and settings; and • Inspection of procedural documentation such as operations manuals, flow charts and job descriptions.
Observation	Observed the implementation, application or existence of specific controls as represented. Observed the relevant processes or procedures during fieldwork. This included, but was not limited to, witnessing the performance of controls or evidence of control performance with relevant personnel, systems, or locations relevant to the performance of control policies and procedures.
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

General Sampling Methodology

Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Prescient Assurance LLC utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, to determine the number of items to be selected in a sample for a particular test. Prescient Assurance LLC, in accordance with AICPA authoritative literature, selected samples in such a way that the samples were expected to be representative of the population. This included judgmental selection methods, where applicable, to ensure representative samples were obtained.

System- generated population listings were obtained whenever possible to ensure completeness prior to selecting samples. In some instances, full populations were tested in cases including, but not limited to, the uniqueness of the event or low overall population size.

Reliability of Information Provided by the Service Organization

Observation and inspection procedures were performed related to certain system-generated reports, listings, and queries to assess the accuracy and completeness (reliability) of the information used in the performance of our testing of the controls.

Test Results

The results of each test applied are listed alongside each respective test applied within the Testing Matrices. Test results not deemed as control deviations are noted by the phrase “No exceptions noted.” in the test result column of the Testing Matrices. Any phrase other than this constitutes either a test result that is the result of non-occurrence, a change in the application of the control activity, or a deficiency in the Operating Effectiveness of the control activity. Testing deviations identified within the Testing Matrices are not necessarily weaknesses in the total system of controls, as this determination can only be made after consideration of controls in place at user entities and subservice organizations, if applicable, and other factors.

Trust ID	Trust Services Criteria	Control Description	Test Applied by the Service Auditor	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company performs reference checks on new employees.	Inspected evidence of reference checks performed for a sample of new employees to determine that the company performed reference checks on new employees.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Inspected the Human Resource Security Policy and Code of conduct to determine that the company requires contractors to acknowledge the same at the time of hire. Inspected the contractor agreements for a sample of new contractors and noted that 1 out the 5 samples tested did not sign the agreement. Hence an exception is noted.	Exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the code of conduct acknowledgement for a sample of new employees and determined that the company required employees to acknowledge a code of conduct at the time of hire. Inspected the code of conduct policy to determine that employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	No exceptions noted.

CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires contractors to sign a confidentiality agreement at the time of engagement.	Inspected the Human Resource Security Policy to determine that the company requires employees to sign confidentiality agreement the time of hire. Inspected the confidentiality agreements for a sample of new contractors and noted that there was no signed confidentiality agreement on record for 4 out the 5 samples tested. Hence an exception is noted.	Exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company requires employees to sign a confidentiality agreement during onboarding.	Inspected the signed confidentiality agreement for a sample of new hires to determine that the company requires employees to sign a confidentiality agreement during onboarding.	No exceptions noted.
CC1.1	The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evidence of performance evaluations performed for a sample of current personnel to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls. The board engages third-party information security experts and consultants as needed.	Inspected the bio for the members of the company's board of directors to determine that the company's board members had sufficient	No exceptions noted.

			expertise to oversee management's ability to design, implement and operate information security controls. Inspected the penetration test report to determine that the board engages third-party information security experts and consultants as needed.	
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors meets at least annually and maintains formal meeting minutes.	Inspected the Board of Directors meeting minutes to determine that the company's board of directors met at least annually and maintained formal meeting minutes.	No exceptions noted.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors or a relevant subcommittee is briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provides feedback and direction to management as needed.	Inspected the board meeting minutes to determine that the company's board of directors or a relevant subcommittee was briefed by senior management at least annually on the state of the company's cybersecurity and privacy risk. The board provided feedback and direction to management as needed.	No exceptions noted.
CC1.2	The Board of Directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Information Security Roles and Responsibilities Policy and Board of Directors Charter to determine that the company's board of directors had a documented	No exceptions noted.

			charter that outlines its oversight responsibilities for internal control.	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management had established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company's board of directors has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the Information Security Roles and Responsibilities Policy and Board of Directors Charter to determine that the company's board of directors had a documented charter that outlines its oversight responsibilities for internal control.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	The company maintains an organizational chart that describes the organizational structure and reporting lines.	Inspected the organizational chart to determine that the company maintained an organizational chart that describes the organizational structure and reporting lines.	No exceptions noted.
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions for key security roles to determine that roles and	No exceptions noted.

			responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected evidence of completed security awareness training for a sample of new hires to determine that the company required employees to complete security awareness training within thirty days of hire. Inspected evidence of completed security awareness training for a sample of current personnel to determine that the company required employees to complete security awareness training at least annually.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs reference checks on new employees.	Inspected evidence of reference checks performed for a sample of new employees to determine that the company performed reference checks on new employees.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and	Inspected the Information Security Roles and Responsibilities Policy and job descriptions for key security roles to	No exceptions noted.

		Responsibilities policy.	determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evidence of performance evaluations performed for a sample of current personnel to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions for key security roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.

CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company managers are required to complete performance evaluations for direct reports at least annually.	Inspected evidence of performance evaluations performed for a sample of current personnel to determine that the company managers were required to complete performance evaluations for direct reports at least annually.	No exceptions noted.
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Inspected the code of conduct acknowledgement for a sample of new employees and determined that the company required employees to acknowledge a code of conduct at the time of hire. Inspected the code of conduct policy to determine that employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	No exceptions noted.
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA	Inspected the control dashboard to determine that the company performed control self-assessments at least annually to	No exceptions noted.

		for a finding, the corrective action is completed within that SLA.	gain assurance that controls were in place and operating effectively. Corrective actions were taken based on relevant findings. If the company had committed to an SLA for a finding, the corrective action was completed within that SLA.	
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company website documentation page to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed at least annually.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has established a formalized whistleblower policy, and an anonymous communication channel is in place for users to report potential issues or fraud concerns.	Inspected the Information Security Policy and whistleblower form to determine that the company had established a	No exceptions noted.

			formalized whistleblower policy, and an anonymous communication channel was in place for users to report potential issues or fraud concerns.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Roles and Responsibilities Policy to determine that the company management had established defined roles and responsibilities to oversee the design and implementation of information security controls.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company communicates system changes to authorized internal users.	Inspected internal communications to determine that the company communicated system changes to authorized internal users.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company requires employees to complete security awareness training within thirty days of hire and at least annually thereafter.	Inspected evidence of completed security awareness training for a sample of new hires to determine that the company required employees to complete security awareness training within thirty days of hire. Inspected evidence of completed security awareness training for a sample of current personnel to determine that the company required employees to complete security awareness training	No exceptions noted.

			at least annually.	
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions for key security roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan policy and Incident Response Plan acknowledgements to determine that the company had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides guidelines and technical support resources relating to system operations to customers.	Inspected the company website help center to determine that the company provides guidelines and technical support resources relating to system operations to customers.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the	The company's security commitments are communicated to customers in Master Service	Inspected the company's terms of service to	No exceptions noted.

	functioning of internal control.	Agreements (MSA) or Terms of Service (TOS).	determine that the company's security commitments were communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Inspected the company's website help center and contact us portals to determine that the company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company notifies customers of critical system changes that may affect their processing.	Inspected external communications to determine that the company notified customers of critical system changes that may affect their processing.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company provides a description of its products and services to internal and external users.	Inspected the company website documentation page to determine that the company provides a description of its products and services to internal and external users.	No exceptions noted.
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include security commitments applicable to that entity.	Inspected the service agreements for a sample of vendors to determine that the company has written agreements in place with vendors and related third-parties. These	No exceptions noted.

			agreements included security commitments applicable to that entity.	
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy and 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.
CC3.2	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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and a sample of vendor compliance reports to determine that the company had a vendor management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements, and - review of critical third-party vendors at least annually.	No exceptions noted.

CC3.2	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.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC3.2	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.	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 risk assessment to determine that 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.	No exceptions noted.
CC3.2	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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery (BC/DR) Policy and the BCDR Exercise Report to determine that the company had a documented business	No exceptions noted.

			continuity/disaster recovery (BC/DR) plan and tested it at least annually.	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 risk assessment to determine that 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.	No exceptions noted.
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and remediation ticket to determine that the company's	No exceptions noted.

			penetration testing was performed at least annually and a remediation plan was developed and changes were implemented to remediate vulnerabilities in accordance with SLAs.	
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's CI/CD pipeline dashboard 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.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.	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 risk assessment to determine that 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.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system	The company has a documented risk management program in place that includes guidance on the	Inspected the Risk Management Policy to determine	No exceptions noted.

	of internal control.	identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	that the company had 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.	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control dashboard to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively. Corrective actions were taken based on relevant findings. If the company had committed to an SLA for a finding, the corrective action was completed within that SLA.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems.	No exceptions noted.
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and remediation ticket to determine that the company's penetration testing was performed at	No exceptions noted.

			least annually and a remediation plan was developed and changes were implemented to remediate vulnerabilities in accordance with SLAs.	
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and a sample of vendor compliance reports to determine that the company had a vendor management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements, and - review of critical third-party vendors at least annually.	No exceptions noted.
CC4.2	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.	The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings. If the company has committed to an SLA for a finding, the corrective action is completed within that SLA.	Inspected the control dashboard to determine that the company performed control self-assessments at least annually to gain assurance that controls were in place and operating effectively. Corrective actions were taken based on relevant findings. If the company had committed to an SLA for a finding, the corrective action was completed within that SLA.	No exceptions noted.
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security requirements; and - review of	Inspected the vendor inventory and a sample of vendor compliance reports to determine that the	No exceptions noted.

	and The Board of Directors, as appropriate.	critical third-party vendors at least annually.	company had a vendor management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements, and - review of critical third-party vendors at least annually.	
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed at least annually.	No exceptions noted.
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	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 Secure Development Policy to determine that the company had a formal systems development life cycle (SDLC) methodology in place that governs the development,	No exceptions noted.

			acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures were documented and reviewed at least annually.	No exceptions noted.
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company's 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 Access Control Policy to determine that the company's access control policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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 Management Policy 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development,	Inspected the Secure Development Policy to determine that	No exceptions noted.

	into action.	acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	the company had 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.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected change tickets for a sample of software and infrastructure changes implemented during the period to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and a sample of vendor compliance reports to determine that the company had a vendor management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements, and - review of critical	No exceptions noted.

			third-party vendors at least annually.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Data Management Policy and Operations Security Policy to determine that the company's data backup policy documented requirements for backup and recovery of customer data.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Inspected the Risk Management Policy and 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.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected the company's information security policies and procedures to determine that the company's information security policies and procedures	No exceptions noted.

			were documented and reviewed at least annually.	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan policy and Incident Response Plan acknowledgements to determine that the company had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Inspected the Information Security Roles and Responsibilities Policy and job descriptions for key security roles to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls were formally assigned in job descriptions and/or the Roles and Responsibilities policy.	No exceptions noted.
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.	The company requires passwords for in-scope system components to be configured according to the company's policy.	Inspected the Access control policy and password configurations to determine that the company requires passwords for in-scope system components to be configured according to the company's policy.	Exceptions noted.

			The service auditor noted that the password was not configured as per Access Control Policy. Hence, an exception is noted.	
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.	The company requires authentication to systems and applications to use unique username and password or MFA.	Inspected the user listings and MFA configurations to determine that the company required authentication to systems and applications to use unique username and password or MFA.	No exceptions noted.
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.	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 Data Management 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	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.	System access restricted to authorized access only.	Inspected the user listings for all in-scope systems to determine that system access was restricted to authorized access only.	No exceptions noted.
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.	The company restricts privileged access to databases to authorized users with a business need.	Inspected database user listings to determine that the company restricted privileged access to databases to authorized users with a business need.	No exceptions noted.
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	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the access listings of firewall systems to determine that the company restricted privileged access	No exceptions noted.

	entity's objectives.		to the firewall to authorized users with a business need.	
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.	The company restricts privileged access to the operating system to authorized users with a business need.	Inspected operating system user listings to determine that the company restricted privileged access to the operating system to authorized users with a business need.	No exceptions noted.
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.	The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as MFA.	Inspected the MFA configurations of production datastores to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms, such as MFA.	No exceptions noted.
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.	The company restricts privileged access to the production network to authorized users with a business need.	Inspected production network user listings to determine that the company restricted privileged access to the production network to authorized users with a business need.	No exceptions noted.
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.	The company requires authentication to the "production network" to use unique usernames and passwords or MFA.	Inspected the Access Control Policy and user listings to determine that the company required authentication to the "production network" to use unique usernames and passwords or MFA.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted	Inspected the encryption configuration to determine that the	No exceptions noted.

	assets to protect them from security events to meet the entity's objectives.	connection.	company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	
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.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the network segmentation evidence to determine that the company's network was segmented to prevent unauthorized access to customer data.	No exceptions noted.
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.	The company maintains a formal inventory of production system assets.	Inspected the asset inventory to determine that the company maintained a formal inventory of production system assets.	No exceptions noted.
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.	The company restricts privileged access to encryption keys to authorized users with a business need.	Inspected the listing of users with privileged access to encryption keys to determine that the company restricted privileged access to encryption keys to authorized users with a business need.	No exceptions noted.
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.	The company's datastores housing sensitive customer data are encrypted at rest.	Inspected encryption configurations to determine that the company's datastores housing sensitive customer data were encrypted at rest.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form	Inspected the access review and user listings to determine that the company ensured	No exceptions noted.

	security events to meet the entity's objectives.	and manager approval prior to access being provisioned.	that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	
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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the access user listings to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
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.	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 of production system to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
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.	The company's 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 Access Control Policy to determine that the company's access control policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC6.2	Prior to issuing system credentials and granting system access, the entity registers and	The company conducts access reviews at least quarterly for the in-scope system components to help	Inspected access reviews to determine that the	No exceptions noted.

	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.	ensure that access is restricted appropriately. Required changes are tracked to completion.	company conducted access reviews at least quarterly for the in-scope system components to help ensure that access was restricted appropriately.	
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.	The company requires authentication to the "production network" to use unique usernames and passwords or MFA.	Inspected the Access Control Policy and user listings to determine that the company required authentication to the "production network" to use unique usernames and passwords or MFA.	No exceptions noted.
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.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access review and user listings to determine that the company ensured that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
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.	The company's 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 Access Control Policy to determine that the company's access control policy documented the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC6.2	Prior to issuing system	The company completes	Inspected	No

	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.	termination checklists to ensure that access is revoked for terminated employees within SLAs.	termination checklists for a sample of terminated personnel to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	exceptions noted.
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company requires authentication to the "production network" to use unique usernames and passwords or MFA.	Inspected the Access Control Policy and user listings to determine that the company required authentication to the "production network" to use unique usernames and passwords or MFA.	No exceptions noted.
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Inspected the access review and user listings to determine that the company ensured that user access to in-scope system components was based on job role and function or required a documented access request form and manager approval prior to access being provisioned.	No exceptions noted.
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company's 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 Access Control Policy to determine that the company's access control policy documented the requirements for the following access control functions: - adding new users; - modifying users;	No exceptions noted.

			and/or - removing an existing user's access..	
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected termination checklists for a sample of terminated personnel to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	No exceptions noted.
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, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected access reviews to determine that the company conducted access reviews at least quarterly for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
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.	The company conducts access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Inspected access reviews to determine that the company conducted access reviews at least quarterly for the in-scope system components to help ensure that access was restricted appropriately.	No exceptions noted.
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.	The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Inspected the Data Management Policy to determine that the company purges or removes customer data containing confidential information from the application	Not tested. Control activity did not occur during the audit period.

			environment, in accordance with best practices, when customers leave the service. Inquired with company management to determine that no customers left the service during the audit period.	
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.	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 Management Policy 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	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.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected termination checklists for a sample of terminated personnel to determine that the company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	No exceptions noted.
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.	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Inspected the asset management policy to determine that the company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Not tested. Control activity did not occur during the audit period.

			Inquired with company management to determine no devices disposals occurred during the audit period.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company requires authentication to the "production network" to use unique usernames and passwords or MFA.	Inspected the Access Control Policy and user listings to determine that the company required authentication to the "production network" to use unique usernames and passwords or MFA.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Inspected the firewall review document to determine that the company reviewed its firewall rulesets at least annually. Required changes were tracked to completion.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the intrusion detection system configurations to determine that the company used an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the website encryption certificate to determine that the company used secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public	No exceptions noted.

			networks.	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company uses firewalls and configures them to prevent unauthorized access.	Inspected the firewall configurations to determine that the company used firewalls and configured them to prevent unauthorized access.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	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 of production system to determine that the company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that the company's network and system hardening standards were documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected the encryption configuration to determine that the company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	No exceptions noted.
CC6.6	The entity implements logical access security measures to protect against threats from	The company has infrastructure supporting the service patched as a part of routine maintenance and	Inspected the patching evidence to determine that	No exceptions noted.

	sources outside its system boundaries.	as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	
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.	The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Inspected the MDM configurations to determine that the company had a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
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.	The company encrypts portable and removable media devices when used.	Inspected the encryption configurations for a sample of workstations and removable media configurations to determine that the company encrypts portable and removable media devices when used.	No exceptions noted.
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.	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Inspected the website encryption 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.
CC6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation,	Inspected the Secure Development Policy to determine that the company had a	No exceptions noted.

	objectives.	changes (including emergency changes), and maintenance of information systems and related technology requirements.	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.	
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.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Inspected the anti-malware deployment for a sample of current employee workstations to determine that the company deployed anti-malware technology to environments commonly susceptible to malicious attacks and configured them to be updated routinely, logged, and installed on all relevant systems.	No exceptions noted.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patching evidence to determine that the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability	Inspected the Operations Security Policy to determine that the company's	No exceptions noted.

	result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	management; - system monitoring.	formal policies outlined the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	
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.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the company's CI/CD pipeline dashboard 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	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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected change tickets for a sample of software and infrastructure changes implemented during the period to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing	No exceptions noted.

			systems.	
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.	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 risk assessment to determine that 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.	No exceptions noted.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patching evidence to determine that the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
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.	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Inspected the log management tool configurations to determine that the company utilized a log management tool to identify events that may have a potential impact on the company's ability to	No exceptions noted.

			achieve its security objectives.	
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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and remediation ticket to determine that the company's penetration testing was performed at least annually and a remediation plan was developed and changes were implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems.	No exceptions noted.
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.	The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the intrusion detection system configurations to determine that the company used an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	No exceptions noted.
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.	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	No exceptions noted.

			predefined thresholds are met.	
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.	The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Inspected the Operations Security 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.
CC7.3	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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan policy and Incident Response Plan acknowledgements to determine that the company had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
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.	The company's security and privacy 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 Incident Response Plan to determine that security and privacy 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. Inquired with company management to determine that no security and privacy incidents occurred during the audit period.	Not tested. Control activity did not occur during the audit period.

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.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan policy and Incident Response Plan acknowledgements to determine that the company had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems.	No exceptions noted.
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.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Inspected the patching evidence to determine that the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	No exceptions noted.
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.	The company's security and privacy 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 Incident Response Plan to determine that security and privacy incidents were logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security	Not tested. Control activity did not occur during the audit period.

			incident response policy and procedures. Inquired with company management to determine that no security and privacy incidents occurred during the audit period.	
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.	The company tests their incident response plan at least annually.	Inspected the Incident response plan and tabletop exercise documentation to determine that the company tested their incident response plan at least annually.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company's security and privacy 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 Incident Response Plan to determine that security and privacy 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. Inquired with company management to determine that no security and privacy incidents occurred during the audit period.	Not tested. Control activity did not occur during the audit period.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company tests their incident response plan at least annually.	Inspected the Incident response plan and tabletop exercise documentation to determine that the company tested their incident response plan at least annually.	No exceptions noted.

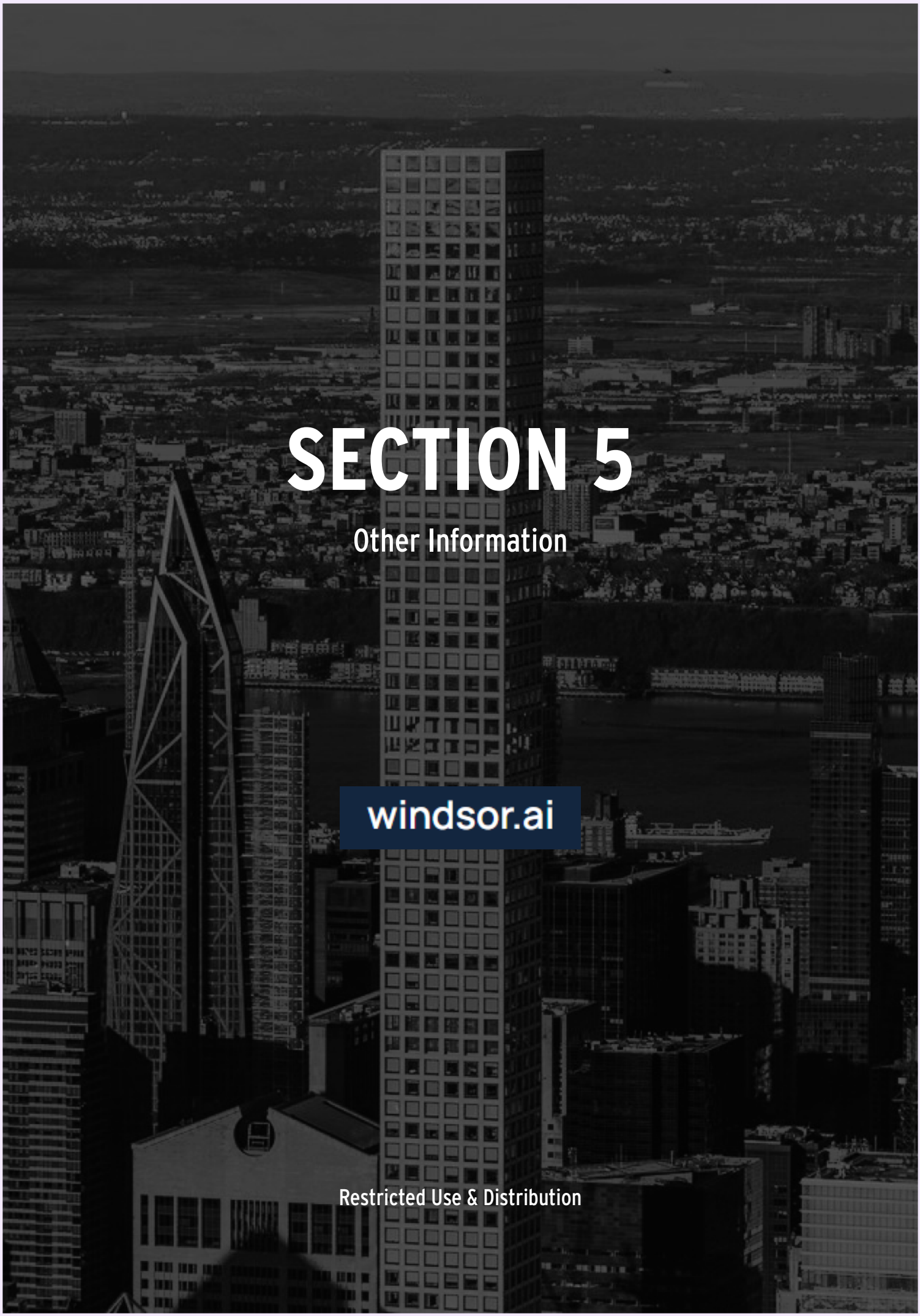
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Inspected the Incident Response Plan policy and Incident Response Plan acknowledgements to determine that the company had security and privacy incident response policies and procedures that were documented and communicated to authorized users.	No exceptions noted.
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the Business Continuity and Disaster Recovery (BC/DR) Policy and the BCDR Exercise Report to determine that the company had a documented business continuity/disaster recovery (BC/DR) plan and tested it at least annually.	No exceptions noted.
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.	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Inspected change tickets for a sample of software and infrastructure changes implemented during the period to determine that the company required changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	No exceptions noted.
CC8.1	The entity authorizes, designs, develops or acquires,	The company has infrastructure supporting the service patched as	Inspected the patching evidence	No exceptions

	configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	to determine that the company had infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service were hardened against security threats.	noted.
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.	The company restricts access to migrate changes to production to authorized personnel.	Inspected the access user listings to determine that the company restricts access to migrate changes to production to authorized personnel.	No exceptions noted.
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.	The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Inspected the Operations Security Policy to determine that the company's network and system hardening standards were documented, based on industry best practices, and reviewed at least annually.	No exceptions noted.
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.	The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Inspected the penetration test report and remediation ticket to determine that the company's penetration testing was performed at least annually and a remediation plan was developed and changes were implemented to remediate vulnerabilities in accordance with SLAs.	No exceptions noted.
CC8.1	The entity authorizes, designs,	The company has a formal	Inspected the	No

	develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	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.	Secure Development Policy to determine that the company had 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.	exceptions noted.
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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked to remediation.	Inspected vulnerability scan results to determine that host-based vulnerability scans were performed at least quarterly on all external-facing systems.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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 Risk Management Policy to determine that the company had 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.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	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	Inspected the annual risk assessment to determine that the company's risk assessments are performed at least	No exceptions noted.

		assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	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.	
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Inspected the Business Continuity and Disaster Recovery Plan to determine that the company had Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	No exceptions noted.
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	Inspected the cybersecurity insurance policy documents to determine that the company maintains cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has written agreements in place with vendors and related third-parties. These agreements include security commitments applicable to that	Inspected the service agreements for a sample of vendors to determine that the	No exceptions noted.

		entity.	company has written agreements in place with vendors and related third-parties. These agreements included security commitments applicable to that entity.	
CC9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory and a sample of vendor compliance reports to determine that the company had a vendor management program in place. Components of this program include: - critical third-party vendor inventory. - vendor's security requirements, and - review of critical third-party vendors at least annually.	No exceptions noted.



SECTION 5

Other Information

windsor.ai

Other Information Provided by Windsor Group AG that is not covered by the Independent Service Auditor's Report

The information in this section is presented by Windsor Group AG to provide additional information to its user entities, business partners, and other specified parties and is not part of Windsor Group AG's description of its system and controls included in Section 3 and Section 4. The evidence has not been subjected to the procedures applied in the examination of the description of Windsor Group AG's system and the suitability of design and operating effectiveness of controls to achieve Windsor Group AG's service commitments and system requirements based on the applicable trust services criteria, and accordingly, Prescient Assurance LLC expresses no opinion on it.

Management's Response to the exception at CC 1.1, 6.1

Control Description:

The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.

Exception noted:

The service auditor noted that one of the five contractors did not sign contractor agreement. Hence, exception noted.

Management's Response:

Windsor Group AG acknowledges the exception identified by the auditor. During the review period, 1 of 5 contractors engaged by the company did not have a signed contractor agreement containing, or referencing, the company's code of conduct. Management agrees with the finding as noted. The exception was caused by a gap in the contractor onboarding process, whereby the specific contractor began providing services before the formal onboarding. This occurred due to a manual, non-automated tracking process and which does not include a systematic checkpoint to prevent service commencement prior to full contract execution.

Management has taken the following corrective actions:

- The affected contractor agreement has been located and executed
- Windsor Group AG is reviewing and revamping the process of employees and contractors onboarding with the help of the HR software.
- Windsor Group AG i has approved the hiring of a full-time HR Manager who will own and execute HR-related documentation, including contractor and employee onboarding

The status of the remediation is in progress. The HR Manager onboarding is scheduled for H2 2026. The implementation of the HR Software has started but is still in progress.

Management's Response to the exception at CC 1.1

Control Description:

The company requires contractors to sign a confidentiality agreement at the time of engagement.

Exception noted:

The service auditor noted that four of the five sampled new hires did not sign a confidentiality agreement.

Management's Response:

Windsor Group AG engages a portion of its contractors through the Upwork freelance platform, which includes its own contractual framework containing confidentiality provisions between platform users. Management had relied on this platform-level framework as sufficient coverage for confidentiality, and as a result, a separate, direct confidentiality agreement was not consistently executed with the company at the time of engagement. This reliance on the platform's terms, rather than a direct signed agreement, was not aligned with the company's own control requirement and did not include a checkpoint to ensure a company-specific confidentiality agreement was signed regardless of hiring channel.

Management notes that no confidentiality incidents, data breaches, or unauthorized disclosures occurred as a result of this control gap during the period under review.

Management has taken the following corrective actions:

- The contractor onboarding process is being updated to require a signed, company-specific confidentiality agreement for all contractors at the time of engagement, regardless of hiring platform or channel.
- This requirement is being incorporated into the same onboarding checklist and HR software implementation referenced under the related CC1.1 exception, to ensure consistent tracking and enforcement going forward.
- Existing reliance on the Upwork platform's confidentiality terms will continue to serve as an additional, supplementary safeguard, but will no longer be treated as a substitute for the company's own signed agreement requirement.

Status of Remediation is in progress. Confidentiality agreements for the four identified contractors are being collected on a prospective basis, targeted for completion by 31st of July 2026. The updated onboarding requirement and tracking mechanism are targeted for full implementation by 31st of August 2026, aligned with the broader onboarding process improvements noted above.

Management's Response to the exception at CC 6.1

Control Description:

The company requires passwords for in-scope system components to be configured according to the company's policy.

Exception noted:

The service auditor noted that the password was not configured as per Access Control Policy. Hence, exception noted.

Management's Response:

Windsor Group AG acknowledges the exception identified by the auditor. During the review period, it was noted that Google Workspace accounts were not configured with the periodic password expiration (90 days) and password history/reuse restriction (prohibiting reuse of the last 16 passwords) settings required by the company's Access Control Policy. Management agrees with the finding as noted.

The Access Control Policy required passwords to expire every 90 days and prohibited reuse of the last 16 passwords used. However, Google Workspace accounts were not configured to enforce these settings, and the discrepancy between the policy requirement and the actual platform configuration had not been identified through a prior configuration review.

Following the exception being raised, DevOps evaluated the configuration changes needed to enable these settings within Google Workspace. As part of that evaluation, management reviewed current Google Workspace security guidance, which recommends against mandatory periodic password rotation and forced password history/reuse restrictions, in favor of multi-factor authentication (MFA), strong password requirements, and risk-based/anomalous login detection as more effective controls. Based on this evaluation, management determined that updating the Access Control Policy to align with current platform best practices, rather than configuring legacy rotation-based settings, is the more appropriate and durable remediation.

Management will take the following corrective actions:

- The Access Control Policy will be updated to remove the 90-day password expiration and 16-password reuse requirements, and to formally adopt MFA, strong password complexity requirements, and risk-based login monitoring as the approved controls for Google Workspace and other applicable in-scope systems.
- Multi-factor authentication (MFA) has been confirmed as enabled/enforced for all Google Workspace accounts.
- Configuration settings for Google Workspace and other in-scope SaaS platforms have been reviewed to confirm alignment with the revised policy.

Status of Remediation is in progress. The Access Control Policy will be updated and approved by 31st of August 2026, and Google Workspace configuration has been confirmed as consistent with the revised policy. Management will continue to periodically review policy alignment with configuration settings across in-scope systems.