automation consultants including AppFox

SOC 2 Type 2 Report

April 1, 2025 To October 1, 2025

December 10, 2025

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

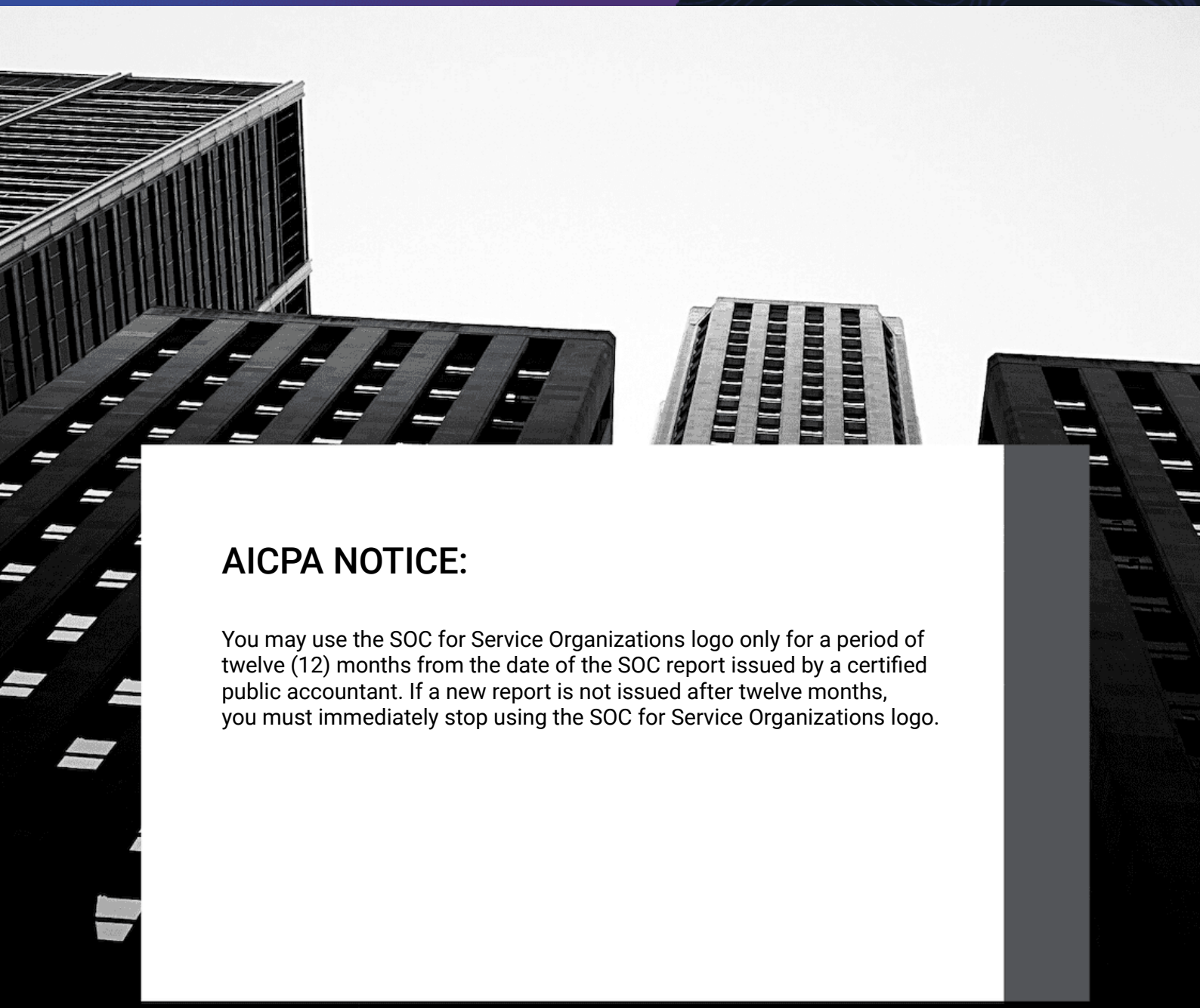
AUDIT AND ATTESTATION BY

PRESCIENT ASSURANCE

AICPA

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

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



AICPA NOTICE:

You may use the SOC for Service Organizations logo only for a period of twelve (12) months from the date of the SOC report issued by a certified public accountant. If a new report is not issued after twelve months, you must immediately stop using the SOC for Service Organizations logo.

Table of Contents

PRESCIENT ASSURANCE

SECTION 1

Management's Assertion

automation consultants
including
AppFox

Management's Assertion

We have prepared the accompanying description of Automation Consultants Ltd's system throughout the period April 01, 2025 to October 01, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report *(With Revised Implementation Guidance—2022).* The description is intended to provide report users with information about Automation Consultants Ltd's system that may be useful when assessing the risks arising from interactions with Automation Consultants Ltd's system, particularly information about system controls that Automation Consultants Ltd 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 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022).*

Automation Consultants Ltd 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 Automation Consultants Ltd, to achieve Automation Consultants Ltd's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Consultants Ltd's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Automation Consultants Ltd'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 Automation Consultants Ltd, to achieve Automation Consultants Ltd's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Consultants Ltd's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Automation Consultants Ltd's controls.

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

1. The description presents Automation Consultants Ltd's system that was designed and implemented throughout the period April 01, 2025 to October 01, 2025 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period April 01, 2025 to October 01, 2025 to provide reasonable assurance that Automation Consultants Ltd's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organization and user entities applied the complementary controls assumed in the design of Automation Consultants Ltd's controls during that period.
3. The controls stated in the description operated effectively throughout the period April 01, 2025, to October 01, 2025, to provide reasonable assurance that Automation Consultants Ltd's service commitments and system requirements were achieved based on the applicable trust services criteria, if the complementary subservice organization and complementary user entity controls assumed in the design of Automation Consultants Ltd's controls operated effectively throughout the period.

David Wakem

David Wakem
Chief Technology Officer
Automation Consultants Ltd

PRESCIENT ASSURANCE

SECTION 2

Independent Service Auditor's Report

Independent Service Auditor's Report

To: Automation Consultants Ltd

Scope

We have examined Automation Consultants Ltd's ("Automation Consultants Ltd") accompanying description of its Entire Company system found in Section 3, titled Automation Consultants Ltd System Description throughout the period April 01, 2025, to October 01, 2025, based on the criteria for a description of a service organization's system set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report *(With Revised Implementation Guidance—2022),* and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 01, 2025, to October 01, 2025, to provide reasonable assurance that Automation Consultants Ltd's service commitments and system requirements were achieved based on the trust services criteria relevant to Security set forth in *TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022).*

Automation Consultants Ltd uses a subservice organization for cloud hosting services and provides application maintenance and support. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Automation Consultants Ltd, to achieve its service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Consultants Ltd's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Automation Consultants Ltd'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 Automation Consultants Ltd, to achieve Automation Consultants Ltd's service commitments and system requirements based on the applicable trust services criteria. The description presents Automation Consultants Ltd's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Automation Consultants Ltd'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

Automation Consultants Ltd 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 Automation Consultants Ltd's service commitments and system requirements were achieved. In Section 1, Automation Consultants Ltd has provided the accompanying assertion titled "Management's Assertion of Automation Consultants Ltd" (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. Automation Consultants Ltd 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 Auditors' 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 operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of 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.

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

Inherent Limitations

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

Opinion

In our opinion, in all material respects:

1. The description presents Automation Consultants Ltd's system that was designed and implemented throughout the period April 01, 2025 to October 01, 2025, in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period April 01, 2025 to October 01, 2025, to provide reasonable assurance that Automation Consultants Ltd's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organization and user entities applied the complementary controls assumed in the design of Automation Consultants Ltd's controls throughout the period.
3. The controls stated in the description operated effectively throughout the period April 01, 2025 to October 01, 2025, to provide reasonable assurance that Automation Consultants Ltd'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 Automation Consultants Ltd's controls operated effectively throughout the 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 Automation Consultants Ltd, user entities of Automation Consultants Ltd's system during some or all of the period April 01, 2025 to October 01, 2025, business partners of Automation Consultants Ltd 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 organisation 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
December 10, 2025

PRESCIENT ASSURANCE

SECTION 3

System Description

automation consultants
including
AppFox

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

Automation Consultants Ltd is a UK company specialising in the provision of IT software solutions. Head Office in Berkshire, UK with subsidiaries in Dublin Ireland, Delaware USA. Customers include Public, Private and Government organisations worldwide.

Description of services overview or services provided

Consultancy service, mostly associated with Atlassian and Monday.com providing installation, configuration, training and migration service. Customer Support for Atlassian systems. Product team, operating under the brand name of AppFox, creating apps for Atlassian and Monday.com

Consultancy service, mostly associated with Atlassian and Monday.com providing installation, configuration, training and migration service. Customer Support for Atlassian systems. Product team, operating under the brand name of AppFox, creating apps for Atlassian and Monday.com

DC 2: The Principal Service Commitments and System Requirements

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

Automation Consultants Ltd commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), online Privacy Police, and commercial contracts

Security commitments

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
- Regular vulnerability scans over the system and network, and 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
- Up time availability of production systems

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

The System description is comprised of the following components:

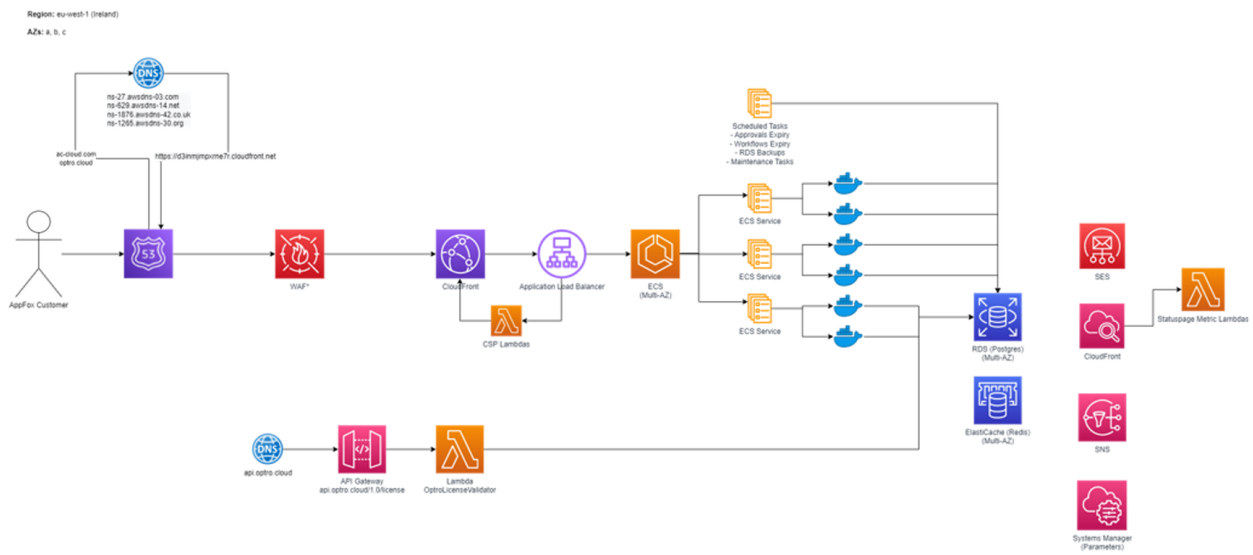
- Software - The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether 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 Infrastructure

Automation Consultants Ltd 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. To outline the topology of its network, the organization maintains the following network diagram(s).



Hardware	Type	Purpose (optional)
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access

Software

Automation Consultants Ltd is responsible for managing the development and operation of the All areas of business operations, including AppFox Development, Consultancy, Managed Services are within scope of SOC 2. system including infrastructure components such as servers, databases, and storage systems. The in-scope Automation Consultants Ltd infrastructure and software components are shown in the table provided below:

System/Application	Purpose
Confluence	A documentation knowledge base
Entra (Office 365)	Identity Management and communications solution
HubSpot	Sales Processing solution

Intune (Microsoft Endpoint Manager)	Mobile Device Management (MDM) for Windows devices
Jamf	Mobile Device Management (MDM) for MacOS devices
Microsoft Defender for Endpoint	Malware and security solution for Windows devices
Personio	HR system
Vanta	Trust Management Solution, containing ISMS, and audit logs of IT security compliance

3.2 People

The company 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. The Company focuses on hiring the right people for the right job as well as training them both on their specific tasks and on the ways to keep the company and its data secure.

Automation Consultants Ltd has a staff of approximately 85 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:

CEO - Francis Miers

CTO/CISO - David Wakem

CHRO - Jarrod Anderson-Cross

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.

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.

3.3 Data

Data as defined by Automation Consultants Ltd, 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 Automation Consultants Ltd

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Automation Consultants Ltd.	Press releases Public website
Internal	Access to internal information is approved by management and is protected from external access.	Internal memos Design documents Product specifications Correspondences
Customer data	Information received from customers for processing or storage by Automation Consultants Ltd. Automation Consultants Ltd must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	Customer operating data Customer PII Customers' customers' PII Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Automation Consultants Ltd to operate the business. Automation Consultants Ltdmust uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	Legal documents Contractual agreements Employee PII Employee salaries

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

All personnel and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, Automation Consultants Ltd has policies and procedures in place to proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.4 Security 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
- Risk Assessment
- Data Retention
- Vendor Management

3.4.1 Physical security

Automation Consultants Ltd's production servers are maintained by Microsoft Azure and AWS. The physical and environmental security protections are the responsibility of Microsoft Azure and AWS. Automation Consultants Ltd reviews the attestation reports and performs a risk analysis of Microsoft Azure and AWS on at least an annual basis.

3.4.2 Logical access

Automation Consultants Ltd provides employees and contracts 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 are 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.

Technology is responsible for provision access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Automation Consultants Ltd's policies, completing security training. These steps must be completed within 14 days of hire.

When an employee is terminated, Technology is responsible for deprovisioning access to all in scope systems within 1 day for that employee's termination.

3.4.3 Computer operations - backups

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

Backup infrastructure is maintained in Microsoft Azure and AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

3.4.4 Computer operations - availability

Automation Consultants Ltd 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.

Automation Consultants Ltd internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

Automation Consultants Ltd 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.

3.4.5 Change management

Automation Consultants Ltd 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 is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. 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 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.

3.4.6 Data communications

Automation Consultants Ltd has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Automation Consultants Ltd 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.

Automation Consultants uses automated monitoring service to perform vulnerability scans, and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities. Issues are resolved by Technology and Development teams using approved change management process

3.5 Boundaries of the system

The boundaries of the Automation Consultants Ltd are the specific aspects of the Company'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 Automation Consultants Ltd. All areas of business operations, including AppFox Development, Consultancy, Managed Services are within scope of SOC 2.

This report does not include the Cloud Hosting Services provided by AWS at multiple facilities. This report does not include the Cloud Hosting Services provided by Azure 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 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 Automation Consultants Ltd's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Automation Consultants Ltd'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:

- Formally, documented organizational policy statements and codes of conduct communicate entity values and behavioral standards to personnel.
- Policies and procedures require employees sign an acknowledgment form indicating they have been given access to the employee manual and understand their responsibility for adhering to the policies and procedures contained within the manual.
- A confidentiality statement agreeing not to disclose proprietary or confidential information, including client information, to unauthorized parties is a component of the employee handbook.
- Background checks are performed for employees as a component of the hiring process.

5.2 Commitment to competence

Automation Consultants Ltd'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:

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

5.3 Management's philosophy and operating style

The Automation Consultants Ltd management team must balance two competing interests: continuing to grow and develop in a cutting edge, rapidly changing technology space while remaining excellent and conservative stewards of the highly-sensitive data and workflows our customers entrust to us.

The management team meets frequently to be briefed on technology changes that impact the way Automation Consultants Ltd 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 Automation Consultants Ltd 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 our 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:

- Management is periodically briefed on regulatory and industry changes affecting the services provided.
- Executive management meetings are held to discuss major initiatives and issues that affect the business.

5.4 Organizational structure and assignment of authority and responsibility

Automation Consultants Ltd'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.

Automation Consultants Ltd'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:

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

5.5 HR policies and practices

Automation Consultants Ltd's success is founded on sound business ethics, reinforced with a high level of efficiency, integrity, and ethical standards. The result of this success is evidenced by its proven track record for hiring and retaining top quality personnel who ensures the service organization is operating at maximum efficiency. Automation Consultants Ltd'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:

- New employees are required to sign acknowledgment forms for the employee handbook and a confidentiality agreement following new hire orientation on their first day of employment.
- Evaluations for each employee are performed on an annual basis.
- Personnel termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk assessment process

Automation Consultants Ltd's risk assessment process identifies and manages risks that could potentially affect Automation Consultants Ltd's ability to provide reliable and secure services to our customers. As part of this process, Automation Consultants Ltd 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 Automation Consultants Ltd product development process so they can be dealt with predictably and iteratively.

5.7 Integration with risk assessment

The environment in which the system operates; the commitments, agreements, and responsibilities of

Automation Consultants Ltd's system; as well as the nature of the components of the system result in risks that the criteria will not be met. Automation Consultants Ltd 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, Automation Consultants Ltd's management identifies the specific risks that the criteria will not be met and the controls necessary to address those risks.

5.8 Information and communication systems

Information and communication are an integral component of Automation Consultants Ltd'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.

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

Structured data is communicated internally via SaaS applications andproject management tools. Finally, Automation Consultants Ltd uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

5.9 Monitoring controls

Management monitors controls to ensure that they are operating as intended and that controls are modified as conditions change. Automation Consultants Ltd'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.

5.9.1 On-going monitoring

Automation Consultants Ltd'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 Automation Consultants Ltd'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 Automation Consultants Ltd's personnel.

5.10 Reporting deficiencies

Our 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)

Automation Consultants Ltd'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 Automation Consultants Ltd's services to be solely achieved by Automation Consultants Ltd control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Consultants Ltd's.

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.

1. User entities are responsible for understanding and complying with their contractual obligations to Automation Consultants Ltd.
2. User entities are responsible for notifying Automation Consultants Ltd of changes made to technical or administrative contact information.
3. User entities are responsible for maintaining their own system(s) of record.
4. User entities are responsible for ensuring the supervision, management, and control of the use of Automation Consultants Ltd services by their personnel.
5. User entities are responsible for developing their own disaster recovery and business continuity plans that address the inability to access or utilize Automation Consultants Ltd services.
6. User entities are responsible for providing Automation Consultants Ltd with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying Automation Consultants Ltd of any actual or suspected information security breaches, including compromised user accounts, including those used for integrations and secure file transfers.

DC 7: Complementary Subservice Organization Controls (CSOCs)

Automation Consultants Ltd's services are designed with the assumption that certain controls will be implemented by subservice organizations. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to Automation Consultants Ltd's services to be solely achieved by Automation Consultants Ltd control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Automation Consultants Ltd.

The following subservice organization controls have been implemented by Microsoft Azure and AWS and included in this report to provide additional assurance that the trust services criteria are met.

Azure

Category	Criteria	Control
Security	CC 6.4	Procedures to restrict physical access to the datacenter to authorized employees, vendors, contractors, and visitors, have been established.
Security	CC 6.4	Security verification and check-in

		for personnel requiring temporary access to the interior of the datacenter facility, including tour groups or visitors, are required.
Security	CC 6.4	Physical access to the datacenter is reviewed quarterly and verified by the Datacenter Management team.
Security	CC 6.4	Physical access mechanisms (e.g., access card readers, biometric devices, man traps / portals, cages, locked cabinets) have been implemented and are administered to restrict access to authorized individuals.
Security	CC 6.4	The datacenter facility is monitored 24x7 by security personnel.
Security	CC 7.2	Azure is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
Security	CC 7.2	Azure is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
Security	CC 7.2	Azure is responsible for overseeing the regular maintenance of environmental protections at data centers.

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
Security	CC 6.4	Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
Security	CC 6.4	Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
Security	CC 6.4	Closed circuit television camera

		(CCTV) are used to monitor server locations in data centers. Images are retained for 90 days, unless limited by legal or contractual obligations.
Security	CC 6.4	Access to server locations is managed by electronic access control devices.
Security	CC 7.2	AWS is responsible for the installation of fire suppression and detection, and environmental monitoring systems at the data centers.
Security	CC 7.2	AWS is responsible for protecting data centers against disruption in power supply to the processing environment by an uninterruptible power supply.
Security	CC 7.2	AWS is responsible for overseeing the regular maintenance of environmental protections at data centers.

Automation Consultants Ltd management, along with the subservice provider, define the scope and responsibility of the controls necessary to meet all the relevant trust services criteria through written contracts, such as service level agreements. In addition, Automation Consultants Ltd performs monitoring of the subservice organization controls, including the following procedures:

- Reviewing and reconciling output reports
- Holding periodic discussions with vendors and subservice organization(s)
- Making regular site visits to vendor and subservice organization(s') facilities
- Testing controls performed by vendors and subservice organization(s)
- Reviewing attestation reports over services provided by vendors and subservice organization(s)
- Monitoring external communications, such as customer complaints relevant to the services by the subservice organization

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

All Common Criteria/Security, Security criteria were applicable to the Automation Consultants Ltd's All areas of business operations, including AppFox Development, Consultancy, Managed Services are within scope of SOC 2. system.

DC 9: Disclosures of Significant Changes in the Last 1 Year

1. **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.
2. **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.

PRESCIENT ASSURANCE

SECTION 4

Testing Matrices

Tests of Operating Effectiveness and Results of Tests

Scope of Testing

This report on the controls relates to Automation Consultants SaaS Platform provided by Automation Consultants Ltd. The scope of the testing was restricted to Entire Company, and its boundaries as defined in Section 3.

Prescient Assurance LLC conducted the examination testing throughout the period April 01, 2025, to October 01, 2025

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 review date. 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.
- Whether the control is manually performed or automated.

Types of Tests Generally Performed

The table below describes the nature of our 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: • Examination / Inspection of source documentation and authorizations to verify transactions processed. • Examination / Inspection of documents or records for evidence of performance, such as existence of initials or signatures. • Examination / Inspection of systems documentation, configurations, and settings; and. • Examination / 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 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, 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 background checks on new employees.	Inspected evidence of background checks performed for a sample of new hires to determine that the company performed background 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 contractor agreements for a sample of contractors onboarded during the audit period to determine that the company required contractor agreements to include a code of conduct or reference to the company code of conduct.	No 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 hires and determined that the company required employees to acknowledge a code of conduct at the time of hire.	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 signed confidentiality agreement for a sample of contractors onboarded during the audit period to determine that the company required contractors to sign	No exceptions noted.

			a confidentiality agreement at the time of engagement.	
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 required employees to signa 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 employees 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 have sufficient expertise to oversee management's ability to design, implement and operate information security controls. Inspected the penetration test and it's results to determine that the board engages	No exceptions noted.

			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 has a documented charter that outlines its oversight responsibilities for internal control.	Inspected the information security roles and responsibilities policy and board meeting minutes to determine that the company's board of directors had a documented charter that outlined its oversight responsibilities for internal control.	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 Management Review Meeting Agenda to determine that 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.	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 meets at least annually and maintains formal meeting minutes. The board includes directors that are independent of the company.	Inspected the meeting minutes to determine that the company's board of directors meet at least annually and maintained formal meeting minutes. Inspected the bio for the members of the company's board of directors	No exceptions noted.

			to determine that the board of directors included directors that are independent of the company.	
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 meeting minutes to determine that the company's board of directors had a documented charter that outlined 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.	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 to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Roles and Responsibilities policy.	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	The company management has	Inspected the	No exceptions

	board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	established defined roles and responsibilities to oversee the design and implementation of information security controls.	Information Security Policy and Information Security Roles and Responsibilities to determine that the company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	noted.
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 employees to determine that the company managers were required to complete performance evaluations for direct reports 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 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 employees to determine that the company required employees to	No exceptions noted.

			complete security awareness training at least annually.	
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 Responsibilities policy.	Inspected the Information Security Roles and Responsibilities policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Roles and Responsibilities policy.	No exceptions noted.
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	The company performs background checks on new employees.	Inspected evidence of background checks performed for a sample of new hires to determine that the company performed background checks on new employees.	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 employees 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	Inspected the Information Security Roles and Responsibilities	No exceptions noted.

		controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	policy to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Roles and Responsibilities policy.	
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 hires and determined that the company required employees to acknowledge a code of conduct at the time of hire.	No exceptions noted.
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. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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	Inspected the control section within Vanta to determine that the company performs	No exceptions noted.

		findings.	control self-assessments at least annually to gain assurance that controls are in place and operation effectively and that corrective actions are taken based on relevant findings.	
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 automated tests 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.
CC2.2	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 product documentation website to determine that the company provided 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 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 procedures to determine that the company has security and privacy incident response policies and procedures that are documented and communicated to authorized 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 communicates system changes to authorized internal users.	Inspected the company's internal communication channels to determine that the company	No exceptions noted.

			communicates system changes to authorized internal users.	
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 whistleblowing policy to determine that 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.	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 company's information security policy to determine that the company's information security policies and procedures are 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 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 employees to determine that the company required employees to complete security	No exceptions noted.

			awareness training 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.	The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Inspected the Information Security Policy and Information Security Roles and Responsibilities to determine that the company management has 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.	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 to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the Roles and Responsibilities policy.	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 company's website 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's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Inspected the customer agreement and Terms of Service to determine that the	No exceptions noted.

			company's security commitments are 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 provides a description of its products and services to internal and external users.	Inspected product documentation website to determine that the company provided 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 provides guidelines and technical support resources relating to system operations to customers.	Inspected the company's user support system 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 functioning of internal control.	The company has written agreements in place with vendors and related third-parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements and determine that the company had written agreements in place with vendors and related third-parties and that these agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
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 user support system to determine that the company has an external-facing support system in place that allows users to report	No exceptions noted.

			system information on failures, incidents, concerns, and other complaints to appropriate personnel.	
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 annual risk assessment and Risk Management Policy to determine that the company specified its objectives to enable the identification and assessment of risk related to the objectives.	No exceptions noted.
CC3.1	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 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.	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 has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated	No exceptions noted.

			with the identified threats, and mitigation strategies for those risks.	
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 assessment was performed at least annually and that the risk assessment included 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 vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory to determine that the company had a vendor management program in place that included a critical third-party vendor invetory, vendor's security and privacy requirements, and a 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 business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Inspected the business continuity and disaster recovery plan policy to determine that the company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	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	Inspected the Risk Management Policy to determine	No exceptions noted.

		identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	that 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.	
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 assessment was performed at least annually and that the risk assessment included 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 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 issue tracking system to determine that 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.	No exceptions noted.
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal	The company has a configuration management procedure in place to ensure that system configurations are	Inspected the CI/ CD deployment dashboards to	No exceptions noted.

	control.	deployed consistently throughout the environment.	determine that the company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	
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 assessment was performed at least annually and that the risk assessment included 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 of internal control.	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 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.	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	Inspected the penetration test report and issue tracking system to determine that the	No exceptions noted.

		accordance with SLAs.	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.	
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.	Inspected the control section within Vanta to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operation effectively and that corrective actions are taken based on relevant findings.	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 has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory to determine that the company had a vendor management program in place that included a critical third-party vendor invetory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	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	No exceptions noted.

			systems. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	
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.	Inspected the control section within Vanta to determine that the company performs control self-assessments at least annually to gain assurance that controls are in place and operation effectively and that corrective actions are taken based on relevant findings.	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 has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory to determine that the company had a vendor management program in place that included a critical third-party vendor invetory, vendor's security and privacy requirements, and a review of critical third-party vendors 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's information security policies and procedures are documented and reviewed at least annually.	Inspected company's information security policy to determine that the company's information security policies and procedures are documented and	No exceptions noted.

			reviewed 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 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 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.	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 documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC5.2	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 and Operations Security Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including	No exceptions noted.

			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 company's information security policy to determine that the company's information security policies and procedures are documented and reviewed at least annually.	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 has 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 into action.	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 and Operations Security Policy to determine that 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	No exceptions noted.

			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 has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory to determine that the company had a vendor management program in place that included a critical third-party vendor invetory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	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 annual risk assessment and Risk Management Policy 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 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 procedures to determine that the company has security and privacy incident response policies and procedures that are 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.	The company's information security policies and procedures are documented and reviewed at least annually.	Inspected company's information security policy to determine that the company's	No exceptions noted.

			information security policies and procedures are 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's data backup policy documents requirements for backup and recovery of customer data.	Inspected the Operations Security Policy to determine that the company's data backup policy documents 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 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 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.	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 has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the	No exceptions noted.

			risks associated with the identified threats, and mitigation strategies for those risks.	
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 to determine that roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in 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'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 documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC6.1	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 user listings and MFA configurations to determine that the company's production system could only be remotely accessed by authorized employees possessing a valid multi-factor	No exceptions noted.

			authentication (MFA) method.	
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 configurations for migrating changes to production to determine that the company restricted 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 restricts privileged access to encryption keys to authorized users with a business need.	Inspected the Management of Database Encryption Keys and Access Controls to determine that the company restricts 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 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 password configurations to determine that the company required passwords for in-scope system components to be configured according to the company's policy.	No exceptions noted.
CC6.1	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	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Inspected encryption configuration and SSL certificate to determine that the company's	No exceptions noted.

	objectives.		production systems could 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 maintains a formal inventory of production system assets.	Inspected the inventory list to determine that the company maintains 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 requires authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	Inspected user listings and configurations to determine that the company required authentication to production datastores to use authorized secure authentication mechanisms, such as unique SSH key.	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 has a data classification policy in place to help ensure that confidential data is 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.	The company's network is segmented to prevent unauthorized access to customer data.	Inspected the Segregation of Environments Policy to determine that the company's network is 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.	System access restricted to authorized access only	Inspected user listings 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 the AWS accounts reviewed to determine that the company restricts 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 entity's objectives.	The company restricts privileged access to the firewall to authorized users with a business need.	Inspected the automated tests to determine that the company restricted privileged access to the firewall 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 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 the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected user listings and configuration to determine that the company required authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.1	The entity implements logical access security software, infrastructure, and architectures	The company restricts privileged access to the production network to authorized users with a business	Inspected production network user listings to	No exceptions noted.

	over protected information assets to protect them from security events to meet the entity's objectives.	need.	determine that the company restricted privileged access to the production network 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 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 new hire access provisioning evidence to determine that the company ensured 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.	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 systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	Inspected user listings and configurations to determine that the company required authentication to systems and applications to use unique username and password or authorized Secure Socket Shell (SSH) keys.	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 requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected user listings and configuration to determine that the company required authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	No exceptions noted.
CC6.2	Prior to issuing system	The company completes termination	Inspected	No exceptions

	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.	checklists to ensure that access is revoked for terminated employees within SLAs.	termination checklists for a sample of terminated employees to determine that the company completed termination checklists to ensure that access is revoked for terminated employees within SLAs.	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 documents 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 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 new hire access provisioning evidence to determine that the company ensured 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.	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	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	Inspected access reviews and resulting access change requests to determine that the	No exceptions noted.

	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.	tracked to completion.	company conducted access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately and that required changes are tracked to completion.	
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 new hire access provisioning evidence to determine that the company ensured 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.	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 documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access..	No exceptions noted.
CC6.3	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	The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected user listings and configuration to determine that the company required authentication to the "production	No exceptions noted.

	least privilege and segregation of duties, to meet the entity's objectives.		network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	
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 and resulting access change requests to determine that the company conducted access reviews at least quarterly for the in-scope system components to help ensure that access is restricted appropriately and that required changes are tracked to completion.	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 completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Inspected termination checklists for a sample of terminated employees to determine that the company completed termination checklists to ensure that access is revoked for terminated employees within SLAs.	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 and resulting access change requests to determine that the company conducted access reviews at least quarterly for the in-scope system components to help ensure that access is restricted	No exceptions noted.

			appropriately and that required changes are tracked to completion.	
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 employees to determine that the company completed 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.	Inquired the client to confirm that no electronic media containing confidential information purged or destroyed during the observation window.	Not tested. No media containing confidential data was purged or destroyed.
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.	Inquired the client to determine that there were no requests for data deletion from the customers during the observation window.	Not tested. No data deletion request during the observation window
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 has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	No exceptions noted.
CC6.6	The entity implements logical	The company's production systems	Inspected	No exceptions

	access security measures to protect against threats from sources outside its system boundaries.	can only be remotely accessed by authorized employees via an approved encrypted connection.	encryption configuration and SSL certificate to determine that the company's production systems could only be remotely accessed by authorized employees via an approved encrypted connection.	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 user listings and MFA configurations to determine that the company's production system could 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 uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Inspected the user sign in logs to determine that the company uses 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 SSL certificate to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	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 firewalls and configures them to prevent unauthorized access.	Inspected the firewall configuration evidence to determine that the company uses firewalls and configures 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 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 are 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 requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Inspected user listings and configuration to determine that the company required authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	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 ruleset review documentation to determine that the company reviews its firewall rulesets at least annually. Required changes are 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 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	Inspected the vulnerability remediation history and SLA misses to determine that the	No exceptions noted.

		the service are hardened against security threats.	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.	
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 SSL certificate to determine that the company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	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 and system architecture documentation 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 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 has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	No exceptions noted.
CC6.8	The entity implements controls to prevent or detect and act upon the	The company deploys anti-malware technology to environments	Inspected the anti-malware	No exceptions noted.

	introduction of unauthorized or malicious software to meet the entity's objectives.	commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	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 configures them to be updated routinely, logged, and installed on all relevant systems.	
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 vulnerability remediation history and SLA misses to determine that 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.	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 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 and Operations Security Policy to determine that the company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency	No exceptions noted.

			changes), and maintenance of information systems and related technology requirements.	
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 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 outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring..	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 has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Inspected the CI/CD deployment dashboards to determine that the company has a configuration management procedure in place to ensure that system configurations are 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'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 assessment was performed at least annually and that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	No exceptions noted.
CC7.1	To meet its objectives, the entity	The company requires changes to	Inspected change	No exceptions

	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.	software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	tickets for a sample of software and infrastructure changes implemented during the period to determine that 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.	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 systems. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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 vulnerability remediation history and SLA misses to determine that the company has infrastructure supporting the service patched as a part of routine maintenance and as a result of	No exceptions noted.

			identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	
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. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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'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 issue tracking system to determine that 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.	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 automated tests to determine that the company utilized a log management tool to identify events that may have a potential impact on the	No exceptions noted.

			company's ability to 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 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 outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring..	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 screenshot to determine that an infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	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 user sign in logs to determine that the company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	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 procedures to determine that the company has security and privacy incident response policies and procedures	No exceptions noted.

			that are documented and communicated to authorized users.	
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.	Inquired with the client to determine that no security or privacy related incidents occurred during the observation window.	Not tested. No security or privacy related incidents occurred during the observation window.
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.	Inquired with the client to determine that no security or privacy related incidents occurred during the observation window.	Not tested. No security or privacy related incidents occurred during the observation window.
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 procedures to determine that the company has security and privacy incident response policies and procedures that are 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.	The company tests their incident response plan at least annually.	Inspected the incident response plan policy and incident response plan procedures to determine that the company tests their incident response plan at least annually.	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 vulnerability remediation history and SLA misses to determine that the company has infrastructure	No exceptions noted.

			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.	
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. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	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 procedures to determine that the company has security and privacy incident response policies and procedures that are 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 plan policy to determine that the company	No exceptions noted.

			has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	
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.	Inquired with the client to determine that no security or privacy related incidents occurred during the observation window.	Not tested. No security or privacy related incidents occurred during the observation window.
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 policy and incident response plan procedures to determine that the company tests their incident response plan 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 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.	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.	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	No exceptions noted.

			were performed at least quarterly on all external-facing systems. Inspected evidence of remediation for a sample of critical and high vulnerabilities to determine that critical and high vulnerabilities were tracked to remediation.	
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 configurations for migrating changes to production to determine that the company restricted 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 are 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 issue tracking system to determine that the company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in	No exceptions noted.

			accordance with SLAs.	
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 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 and Operations Security Policy to determine that 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.	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 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 vulnerability remediation history and SLA misses to determine that 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.	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 has a documented risk management program in place that includes	No exceptions noted.

			guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	
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 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 assessment was performed at least annually and that the risk assessment included a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	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 to determine that the company maintained cybersecurity insurance to mitigate the financial impact of business disruptions.	No exceptions noted.
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 has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to	No exceptions noted.

			maintain information security continuity in the event of the unavailability of key personnel.	
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 confidentiality and privacy commitments applicable to that entity.	Inspected the written agreements and determine that the company had written agreements in place with vendors and related third-parties and that these agreements included confidentiality and privacy commitments applicable to that entity.	No exceptions noted.
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 and privacy requirements; and - review of critical third-party vendors at least annually.	Inspected the vendor inventory to determine that the company had a vendor management program in place that included a critical third-party vendor invetory, vendor's security and privacy requirements, and a review of critical third-party vendors at least annually.	No exceptions noted.

Signed and Accepted by

Prescient Assurance

Prescient Assurance LLC

David Wakem

David Wakem

Chief Technology Officer

Automation Consultants Ltd

Certificate of Completion

Document ID: 11b6d43b-3fde-4f21-9218-cd640f32f86a

Document Title: Report

Status: Completed

Name of the Company: Automation Consultants Ltd

Audit Trail

Username	Email	Action	IP Address	Date/Time
Dishant Arya	dishant.arya@prescientsecurity.com	Report Shared with david.wakem@automation-consultants.com	10.0.21.184	2025-12-01 22:33:06
Yamini Upadhyay	yamini.upadhyay@prescientsecurity.com	report Signed by Admin	49.43.26.240	2025-12-10 14:41:11
David Wakem	david.wakem@automation-consultants.com	report Signed by Client	195.180.33.232	2025-12-10 16:10:09

Management Representation Letter

From: Automation Consultants Ltd

To:

Prescient Assurance LLC

1900 Church Street, Suite 300,

Nashville, TN 37203

+1 646 209 7319

info@prescientassurance.com

In connection with your engagement to report on Automation Consultants Ltd's (service organization) description of its Automation Consultants system titled Automation Consultants System Description throughout the period April 01, 2025 to October 01, 2025 (description) based on the criteria set forth in DC 200, 2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022) (2018 description criteria) and the suitability of the design and operating effectiveness of the controls included in the description throughout the period April 01, 2025 to October 01, 2025 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the trust services criteria relevant to "Security" set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus - 2022) (2017 applicable trust services criteria), we recognize that obtaining representations from us concerning the information contained in this letter is a significant procedure in enabling you to form an opinion about whether the description presents the system that was designed and implemented throughout the observation period in accordance with the description criteria and whether the controls stated in the description were suitably designed and operating effectively throughout the period April 01, 2025 to October 01, 2025 to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.

We confirm, to the best of our knowledge and belief, as of December 10, 2025, the date of your report, the following representations made to you during your examination:

1. We are responsible for the preparation and presentation of the description, including the completeness, accuracy, and method of presentation of the description, in accordance with the description criteria and the suitability of the design and operating effectiveness of the controls included in the description to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
2. We also are responsible for our written assertion that accompanies the description of the system, both of which will be provided to you and users of the report. We are responsible for the completeness, accuracy, and method of presentation of the assertion and for having a reasonable basis for it. We reaffirm our assertion attached to the description.
3. We have evaluated the presentation of the description in accordance with the description criteria and the

suitability of the design and operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria, and all relevant matters have been considered and reflected in our evaluation and in our assertion.

4. We have disclosed to you all known matters that may contradict the presentation of the description or the suitability of the design of the controls stated in the description, or our assertion.
5. We have disclosed to you any communications from regulatory agencies, user entities, or others received through the date of this letter affecting the presentation of the description or the suitability of the design or operating effectiveness of the controls included in the description.
6. We are responsible for determining the scope of your examination, including identifying the time period covered by the engagement, services that are the subject of the examination, the system providing the services (including boundaries of the system), and risks relevant to business partners who provide intellectual property or services related to the system.
7. We are responsible for selecting the trust services category(ies) and criteria to be included within the scope of our examination and determining that such criteria are suitable, will be available to the intended users and they are appropriate for our purposes. We are responsible for stating the applicable trust services criteria and related controls in the description. For any additional criteria specified by law, regulation, or another party, we are responsible for identifying that party in the description.
8. We are responsible for determining the effect on our service commitments and system requirements of any services provided to the service organization by other organizations and determining whether those entities are subservice organizations. We are also responsible for determining whether we will use the carve-out method or inclusive method to present information about services provided at any subservice organizations in our description.
9. We are responsible for identifying and analyzing the risks that threaten the achievement of our service commitments and system requirements based on the applicable trust services criteria.
10. We are responsible for designing, implementing, and documenting controls that are suitably designed and operating effectively to provide reasonable assurance that our service commitments and system requirements are achieved based on the applicable trust services criteria.
11. We are responsible for specifying the principal service commitments made to user entities and the system requirements necessary to operate the system and meet commitments to our business partners.
12. We have provided you with the following:
    1. All relevant information and access, as agreed upon in the terms of the engagement, to all information such as records, documentation, service-level agreements, and internal audit or other reports, of which we are aware that is relevant to your examination and our assertion.
    2. Access to additional information you have requested from us for the purpose of the engagement.
    3. Unrestricted access to persons within the appropriate parties from whom you determined was necessary to obtain evidence relevant to your engagement.
13. We believe the effects of uncorrected misstatements (such as discrepancies in the description or deficiencies in the controls described), if any, are immaterial, individually and in the aggregate, to the presentation of the description in accordance with the description criteria or to the suitability of the design or operating effectiveness of the controls stated therein to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria.
14. We have disclosed to you any known events subsequent to the period covered by the description of the system up to the date of this letter that would have a material effect on the presentation of the description or the suitability of the design or operating effectiveness of the controls, or our assertion.
15. We have disclosed to you any instances of noncompliance with laws and regulations, fraud, or uncorrected misstatements attributable to the service organization that are not clearly trivial and that may affect one or more user entities, and whether such incidents have been communicated appropriately to affected user entities.
16. We have disclosed to you any actual, suspected, or alleged fraud or noncompliance with laws or regulations that could adversely affect the description of the service organization's system, the suitability of the design of the controls stated therein, or achievement of its service commitments and system requirements.
17. We also have disclosed to you all instances about which we are aware of the following:
    1. Misstatements and omissions in the description.
    2. Instances in which controls have not been suitably designed or implemented as described.

3. Instances in which controls did not operate effectively or as described

18. We have disclosed to you all identified system incidents that resulted in a significant impairment of the service organization's achievement of its service commitments and system requirements throughout the period April 01, 2025 to October 01, 2025.
19. We have disclosed to you any changes in the controls that are likely to be relevant to report users occurring through the date of this letter.
20. We have responded fully to all inquiries made to us by you during the examination.
21. We understand that your report is intended solely for the use and information of management of the service organization and others within the organization, user entities to which we provide services, and other specified parties who have sufficient knowledge and understanding to consider it, along with other information,if any. We intend to distribute your report only to those specified parties.

We understand that your examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants and was designed for the purpose of expressing an opinion about whether, in all material respects, the description is presented in accordance with the description criteria and whether the controls stated therein were suitably designed and operating effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We also understand that the opinion was based on your examination and that the procedures performed in the examination were limited to those that you considered necessary.

David Wakem

David Wakem

Chief Technology Officer

Automation Consultants Ltd