High Power Consulting, Inc. DBA/Envoc

SOC 2 TYPE 2 REPORT

FOR THE PERIOD
APRIL 01, 2026 TO JUNE 30, 2026

A TYPE 2 INDEPENDENT SERVICE AUDITOR'S REPORT ON
CONTROLS RELEVANT TO
SECURITY, CONFIDENTIALITY, AND AVAILABILITY

AUDIT AND ATTESTATION BY

Securance Pro Assurance PLLC
Thrive to Security

AICPA NOTICE:

You may use the SOC for Service Organizations - Service Organizations Logo only for a period of twelve (12) months following the date of the SOC report issued by a licensed CPA. If after twelve months a new report is not issued, you must immediately cease use of the SOC for Service Organizations - Logo.

TABLE OF CONTENTS

SECTION 1

MANAGEMENT'S ASSERTION

Management Assertion

We have prepared the accompanying description of High Power Consulting, Inc. DBA/Envoc ("High Power Consulting, Inc. DBA/Envoc" or the company) system throughout the period April 01, 2026 to June 30, 2026, 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. The description is intended to provide report users with information about High Power Consulting, Inc. DBA/Envoc's system that may be useful when assessing the risks arising from interactions with High Power Consulting, Inc. DBA/Envoc's system, particularly information about system controls that High Power Consulting, Inc. DBA/Envoc 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, Confidentiality, and Availability set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

High Power Consulting, Inc. DBA/Envoc uses Google Cloud and Microsoft Azure as subservice organizations 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 High Power Consulting, Inc. DBA/Envoc, to achieve High Power Consulting, Inc. DBA/Envoc's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents High Power Consulting, Inc. DBA/Envoc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc, to achieve High Power Consulting, Inc. DBA/Envoc service commitments and system requirements based on the applicable Trust Services Criteria. The description presents High Power Consulting, Inc. DBA/Envoc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of High Power Consulting, Inc. DBA/Envoc's controls.

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

a) The description presents High Power Consulting, Inc. DBA/Envoc's system that was designed and implemented throughout the period April 01, 2026 to June 30, 2026, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period April 01, 2026 to June 30, 2026, to provide reasonable assurance that High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc's controls during that period.

c) The controls stated in the description operated effectively throughout the period April 01, 2026 to June 30, 2026, to provide reasonable assurance that High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc's controls operated effectively throughout the period.

James DuBos *James DuBos*
President
High Power Consulting, Inc. DBA/Envoc

SECTION 2

INDEPENDENT SERVICE AUDITOR'S REPORT

Independent Service Auditor’s Report

To: High Power Consulting, Inc. DBA/Envoc

Scope

We have examined High Power Consulting, Inc. DBA/Envoc (“High Power Consulting, Inc. DBA/Envoc")'s accompanying description of its various system found in Section 3, titled High Power Consulting, Inc. DBA/Envoc System Description throughout the period April 01, 2026 to June 30, 2026, 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, and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 01, 2026 to June 30, 2026, to provide reasonable assurance that High Power Consulting, Inc. DBA/Envoc service commitments and system requirements were achieved based on the Trust Services Criteria relevant to Security, Confidentiality, and Availability set forth in TSP 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy.

High Power Consulting, Inc. DBA/Envoc uses Google Cloud and Microsoft Azure as subservice organizations 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 High Power Consulting, Inc. DBA/Envoc, to achieve its service commitments and system requirements based on the applicable Trust Services Criteria. The description presents High Power Consulting, Inc. DBA/Envoc's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc, to achieve High Power Consulting, Inc. DBA/Envoc's service commitments and system requirements based on the applicable Trust Services Criteria. The description presents High Power Consulting, Inc. DBA/Envoc's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of High Power Consulting, Inc. DBA/Envoc'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

High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc service commitments and system requirements were achieved. In Section 1, High Power Consulting, Inc. DBA/Envoc has provided the accompanying assertion titled “Management’s Assertion of High Power Consulting, Inc. DBA/Envoc” (assertion) about the description and the suitability of design and operating effectiveness of controls stated therein. High Power Consulting, Inc. DBA/Envoc is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable Trust Services Criteria and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization’s service commitments and system requirements.

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the 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:

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 and implemented 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 any system of internal control, including the possibility of human error and the circumvention of controls. Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable Trust Services Criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls tested and the nature, timing, and results of those tests are presented in the section of our report titled "Testing Matrices."

Opinion

In our opinion, in all material respects:

a) The description presents the High Power Consulting, Inc. DBA/Envoc system that was designed and implemented throughout the period April 01, 2026 to June 30, 2026, in accordance with the description criteria.

b) The controls stated in the description were suitably designed throughout the period April 01, 2026 to June 30, 2026, to provide reasonable assurance that High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc's controls throughout the period.

c) The controls stated in the description operated effectively throughout the period April 01, 2026 to June 30, 2026, to provide reasonable assurance that High Power Consulting, Inc. DBA/Envoc's service commitments and system requirements were achieved based on the applicable Trust Services Criteria, if the complementary subservice organization controls and complementary user entity controls assumed in the design of High Power Consulting, Inc. DBA/Envoc's controls operated effectively throughout the period.

Restricted Use

This report is intended solely for the information and use of High Power Consulting, Inc. DBA/Envoc, user entities of High Power Consulting, Inc. DBA/Envoc's system during some or all of the period April 01, 2026 to June 30, 2026, business partners of High Power Consulting, Inc. DBA/Envoc 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, and other parties.
3. Internal control and its limitations.
4. Complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.
5. User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services.
6. The applicable trust services criteria.
7. The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Securance Pro ASSURANCE PLLC

Digitally signed by Securance Pro Assurance PLLC
Date: 2026.07.07 18:30:10 +05'30'

Securance Pro Assurance PLLC
Kalispell, Montana
Firm License No.: PAC-FIRM-LIC-55940

SECTION 3

SYSTEM DESCRIPTION

DC 1: Company Background

Overview of Operations

High Power Consulting, Inc. DBA/Envoc is a SaaS company headquartered in Baton Rouge, Louisiana, that provides technology-first companies with tailor-made business software solutions. Envoc serves forward-thinking enterprises, government agencies, and early-stage entrepreneurs through custom software development, dev team augmentation, mobile app development, technology modernization, customer call center integration, and product strategy consulting. Envoc delivers its own SaaS projects such as Qtopia Scheduler, FaceLock Identity Solutions, and Spotter Inspections, along with customer applications supporting innovation and complex system integration.

Description of Services Provided

High Power Consulting, Inc. DBA/Envoc provides custom business software and SaaS services, including custom software development, mobile app development (native and cross-platform), technology modernization, product strategy consulting, customer call center integration, and development team augmentation. It delivers tailor-made solutions that modernize technology and integrate complex systems for forward-thinking enterprises, government agencies, and early-stage entrepreneurs, supporting innovation and business growth.

Mission & Vision

High Power Consulting, Inc. DBA/Envoc positions its mission around delivering tailor-made business software solutions for technology-first companies, with an emphasis on unleashing innovation, modernizing technology, integrating complex systems, and driving business growth. It envisions a future where forward-thinking enterprises, government agencies, and early-stage entrepreneurs adopt advanced digital services through custom products that streamline operations and expand public-service innovation.

DC 2: Principal service commitments and system requirements

High Power Consulting, Inc. DBA/Envoc designs its processes and procedures related to the system to meet its objectives. Those objectives are based on the service commitments that High Power Consulting, Inc. DBA/Envoc makes to user entities, the laws and regulations that govern its services, and the financial, operational, and compliance requirements that High Power Consulting, Inc. DBA/Envoc has established. The system services are subject to the security, confidentiality, and availability commitments established internally for its services.

Commitments to user entities are documented and communicated in service-level agreements (SLAs) and other customer agreements, as well as in the description of the service offering provided online.

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 annual penetration testing.
- 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
- Uptime availability of production systems

- Implementation of separation of duties (SoD) for sensitive roles and functions

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

- The use of encryption technologies to protect system data both at rest and in transit.
- Confidentiality and non-disclosure agreements with employees, contractors, and third parties; and,
- Confidential information must be used only for the purposes explicitly stated in agreements between High Power Consulting, Inc. DBA/Envoc and user entities

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

- System performance and availability monitoring mechanisms to help ensure the consistent delivery of the system and its components.
- Responding to customer requests in a timely manner.
- Business continuity and disaster recovery plans and,
- Operational procedures supporting the achievement of availability commitments to user entities.

Such requirements are communicated in High Power Consulting, Inc. DBA/Envoc's system policies and procedures, system design documentation, and contracts with customers. Information-security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition to these policies, standard operating procedures are documented on how to carry out specific manual and automated processes required in the operation and development of the system.

DC 3: Components of the System used to provide 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.

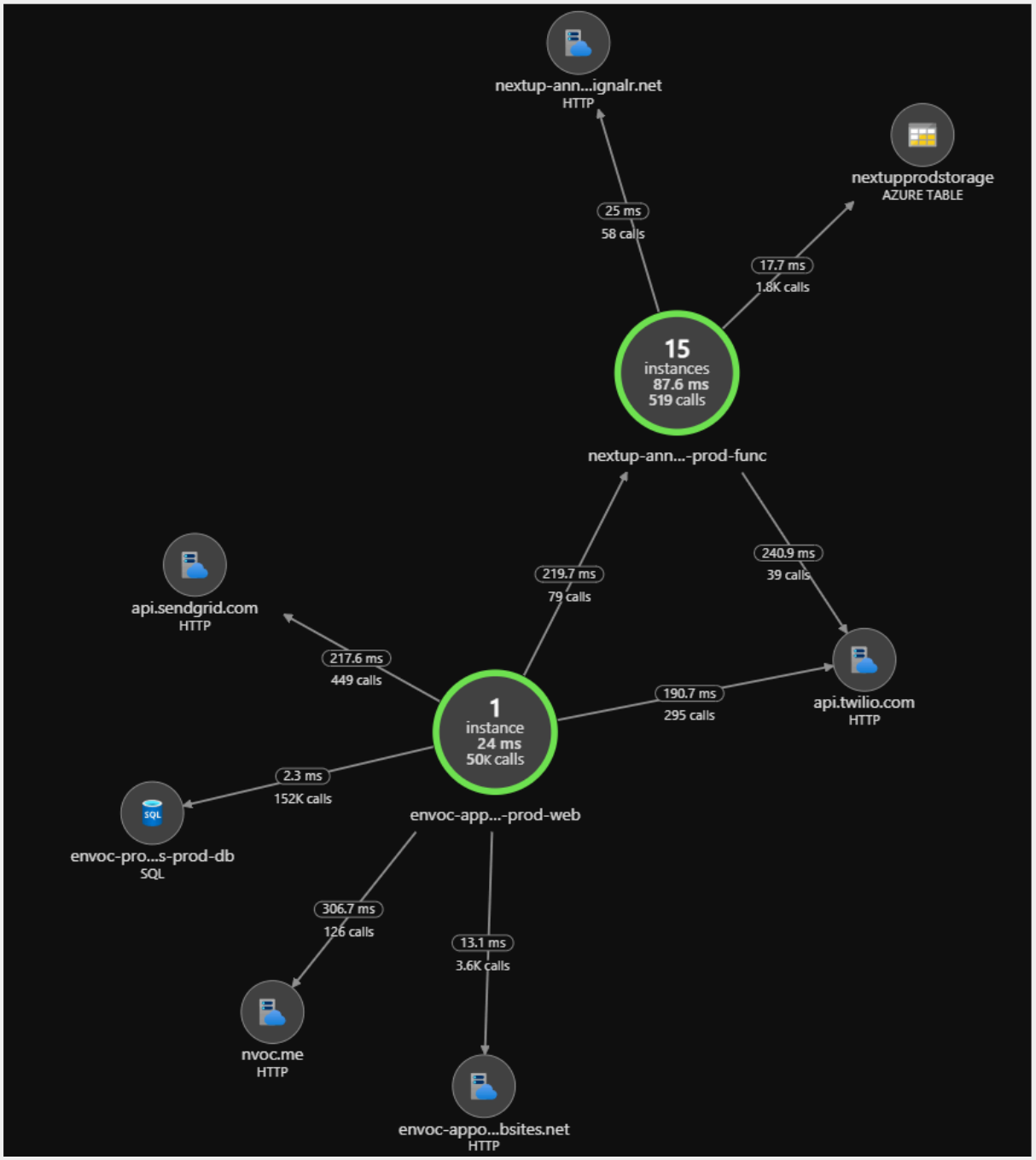
- People - The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).

- 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

High Power Consulting, Inc. DBA/Envoc maintains a system inventory that includes computers (desktops and laptops). 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).



3.2 Software

High Power Consulting, Inc. DBA/Envoc is responsible for managing the development and operation of the High Power Consulting, Inc. DBA/Envoc platform, including infrastructure components such as containers, databases, and storage systems. The in-scope High Power Consulting, Inc. DBA/Envoc infrastructure and software components are shown in the table below:

System/Application	Operating System	Business Function/Description
Google Cloud	IaaS / PaaS	Cloud infrastructure hosting applications and data
Microsoft Azure	IaaS / PaaS	Cloud infrastructure hosting applications and data
Google Workspace	SaaS	Core identity and authentication for team access to work tools
Microsoft 365	SaaS	Core identity and authentication for team access to work tools

3.3 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.

High Power Consulting, Inc. DBA/Envoc has a staff of 24 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.

CEO - Calvin Fabre
COO/President - James DuBos

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

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

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

3.4 Data

Data as defined by High Power Consulting, Inc. DBA/Envoc, 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 High Power Consulting, Inc. DBA/Envoc

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for High Power Consulting, Inc. DBA/Envoc	● 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 High Power Consulting, Inc. DBA/Envoc. High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc to operate the business. High Power Consulting, Inc. DBA/Envoc must 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 and utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, to protect customer data. Additionally, High Power Consulting, Inc. DBA/Envoc has policies and procedures in place to ensure proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

3.5 Processes and procedures

Management has developed and communicated policies and procedures to manage the information security of the system. Changes to these procedures are performed annually and authorized by

management, the executive team, and control owners. These procedures cover the following key security life cycle areas:

- Physical Security
- Logical Access
- Availability
- Change Control
- Data Communications
- Risk Assessment
- Data Retention
- Vendor Management

3.5.1 Physical security

High Power Consulting, Inc. DBA/Envoc's production servers are maintained by Google Cloud and Microsoft Azure. The physical and environmental security protections are the responsibility of Google Cloud and Microsoft Azure. High Power Consulting, Inc. DBA/Envoc reviews the attestation reports and performs a risk analysis of Google Cloud and Microsoft Azure on at least an annual basis.

3.5.2 Logical access

High Power Consulting, Inc. DBA/Envoc provides employees and contractors access to infrastructure via a role-based access control system, to ensure uniform, least privilege access to identified users and to maintain simple and repeatable user provisioning and deprovisioning processes.

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

Developer Operations and Operations are responsible for provisioning access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing High Power Consulting, Inc. DBA/Envoc's policies and completing security training. These steps must be completed within 30 days of hire.

When an employee is terminated, Developer Operations and Operations are responsible for deprovisioning access to all in scope systems within 1 business day of that employee's termination.

3.5.3 Computer operations – backups

Customer data is backed up and monitored by the DevOps for completion and exceptions. If there is an exception, DevOps 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 Google Cloud and Microsoft Azure with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

3.5.4 Computer operations – availability

High Power Consulting, Inc. DBA/Envoc 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.

High Power Consulting, Inc. DBA/Envoc internally monitors all applications, including the web UI, databases, and cloud storage to ensure that service delivery matches SLA requirements.

High Power Consulting, Inc. DBA/Envoc utilizes vulnerability scanning software that checks source code for common security issues as well as for vulnerabilities identified in open source dependencies and maintains an internal SLA for responding to those issues.

3.5.5 Change management

High Power Consulting, Inc. DBA/Envoc 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 by developers.

3.5.6 Data communications

High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 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.

High Power Consulting, Inc. DBA/Envoc uses multiple vulnerability scanning tools to identify security risks that could compromise High Power Consulting, Inc. DBA/Envoc's applications or infrastructure (network devices, databases, and servers). These scans are performed on both High Power Consulting, Inc. DBA/Envoc's internal networks and externally facing networks. Management reviews the results of the scans and works with applicable teams to agree on an appropriate timeframe to apply patches based on the risk posed to the application, the infrastructure, or the network, and whether there is a publicly known exploit.

3.6 Boundaries of the system

The boundaries of the High Power Consulting, Inc. DBA/Envoc system 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 High Power Consulting, Inc. DBA/Envoc.

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

DC 4: Disclosures about identified security incidents

No significant security incidents affecting user entities occurred in the 3 months preceding the review date.

DC 5: Relevant aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

Control Environment

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 High Power Consulting, Inc. DBA/Envoc's control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of High Power Consulting, Inc. DBA/Envoc'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:

- Formal, 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 High Power Consulting, Inc. DBA/Envoc 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

High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 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

High Power Consulting, Inc. DBA/Envoc'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.

High Power Consulting, Inc. DBA/Envoc'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

High Power Consulting, Inc. DBA/Envoc'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 ensure the service organization is operating at maximum efficiency. High Power Consulting, Inc. DBA/Envoc'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 acknowledgement 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.
- Employee termination procedures are in place to guide the termination process and are documented in a termination checklist.

5.6 Risk assessment process

High Power Consulting, Inc. DBA/Envoc's risk assessment process identifies and manages risks that could potentially affect High Power Consulting, Inc. DBA/Envoc's ability to provide reliable and secure services to our customers. As part of this process, High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 's system; as well as the nature of the components of the system result in risks that the criteria will not be met. High Power Consulting, Inc. DBA/Envoc 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, High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc'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.

High Power Consulting, Inc. DBA/Envoc uses several information and communication channels internally to share information with management, employees, contractors, and customers. High Power Consulting, Inc. DBA/Envoc uses chat systems and email as the primary internal and external communications channels.

Structured data is communicated internally via SaaS applications and project management tools. Finally, High Power Consulting, Inc. DBA/Envoc 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. High Power Consulting, Inc. DBA/Envoc'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

High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc'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

High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc's services to be solely achieved by High Power Consulting, Inc. DBA/Envoc control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of High Power Consulting, Inc. DBA/Envoc'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 High Power Consulting, Inc. DBA/Envoc
2. User entities are responsible for notifying High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc 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 High Power Consulting, Inc. DBA/Envoc services.

6. User entities are responsible for providing High Power Consulting, Inc. DBA/Envoc with a list of approvers for security and system configuration changes for data transmission.
7. User entities are responsible for immediately notifying High Power Consulting, Inc. DBA/Envoc 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

High Power Consulting, Inc. DBA/Envoc uses subservice organizations in support of its system. High Power Consulting, Inc. DBA/Envoc's controls related to the system cover only a portion of overall internal control for user entities. It is not feasible for the trust services criteria over High Power Consulting, Inc. DBA/Envoc to be achieved solely by High Power Consulting, Inc. DBA/Envoc. Therefore, user entity controls must be evaluated in conjunction with High Power Consulting, Inc. DBA/Envoc's controls described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

High Power Consulting, Inc. DBA/Envoc periodically reviews the quality of the outsourced operations by various methods including:

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Google Cloud and Microsoft Azure are expected to implement appropriate physical and environmental security controls to protect the infrastructure hosting High Power Consulting, Inc. DBA/Envoc's applications.	Google Cloud and Microsoft Azure	CC6.1, CC6.2
Google Cloud and Microsoft Azure are expected to maintain a robust incident response and notification process, including detection, response, and communication of security events impacting their infrastructure.	Google Cloud and Microsoft Azure	CC7.2, CC7.3
Google Cloud and Microsoft Azure are expected to ensure logical access controls are enforced for systems hosting customer applications, including strong authentication and role-based access.	Google Cloud and Microsoft Azure	CC6.3, CC6.4

Control Activity Expected to be Implemented by Subservice Organization	Subservice Organization	Applicable Criteria
Google Cloud and Microsoft Azure are expected to maintain availability commitments by implementing system monitoring, redundancy, and failover processes.	Google Cloud and Microsoft Azure	CC3.2, A1.2
Google Cloud and Microsoft Azure are expected to conduct regular vulnerability assessments and patch management on their infrastructure components.	Google Cloud and Microsoft Azure	CC7.1, CC8.1
Google Cloud and Microsoft Azure are expected to implement data encryption controls for data in transit and at rest on their hosting platforms.	Google Cloud and Microsoft Azure	CC6.1, C1.1
Google Cloud and Microsoft Azure are expected to have change management processes in place to ensure all infrastructure updates are tested, approved, and tracked.	Google Cloud and Microsoft Azure	CC8.1

High Power Consulting, Inc. DBA/Envoc management, along with the subservice provider, defines 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, High Power Consulting, Inc. DBA/Envoc 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)
- 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: Criteria not applicable to the system

All Common Criteria/Security, Confidentiality, and Availability criteria are applicable to the High Power Consulting, Inc. DBA/Envoc platform.

DC 9: Disclosure of Significant Changes in the Last 3 Months

No significant changes impacting user entities occurred in the 3 months preceding the review date.

SECTION 4

TESTING MATRIX

TESTS OF OPERATING EFFECTIVENESS AND RESULTS OF TESTS

Scope of Testing

This report on the controls relates to the High Power Consulting, Inc. DBA/Envoc System provided by High Power Consulting, Inc. DBA/Envoc. The scope of the testing was restricted to the High Power Consulting, Inc. DBA/Envoc System and its boundaries as defined in Section 3. Securance Pro Assurance PLLC conducted the examination testing over the period April 01, 2026 to June 30, 2026.

Tests of Operating Effectiveness

The tests applied to test the operating effectiveness of controls are listed alongside each of the respective control activities within the Testing Matrices. Such tests were considered necessary to evaluate whether the controls were sufficient to provide reasonable, but not absolute, assurance that the applicable Trust Services Criteria were achieved during the period. In selecting the tests of controls, Securance Pro Assurance PLLC considered various factors including, but not limited to, the following:

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

The types of tests performed with respect to the operational effectiveness of the control activities detailed in this section are briefly described below:

Test Approach	Description
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, emails, web-based conferences, or a combination of the preceding.
Observation	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.
Inspection	Inspected the relevant audit records. This included, but was not limited to, documents, system configurations and settings, or the existence of sampling attributes, such as signatures, approvals, or logged events. In some cases, inspection testing involved tracing events forward to consequent system documentation or processes (e.g., resolution, detailed documentation, alarms, etc.) or vouching backwards for prerequisite events (e.g., approvals, authorizations, etc.).
Re-performance	Re-performed the control to verify the design and / or operation of the control activity as performed if applicable.

Sampling
Consistent with American Institute of Certified Public Accountants (AICPA) authoritative literature, Securance Pro Assurance PLLC utilizes professional judgment to consider the tolerable deviation rate, the expected deviation rate, the audit risk, the characteristics of the population, and other factors, in order to determine the number of items to be selected in a sample for a particular test. Securance Pro Assurance PLLC, 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 the aforementioned, 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. Control considerations that should be implemented by subservice organizations, in order to complement the control activities and achieve the service commitments and system requirements, are presented in the “Subservice Organizations” section within Section 3.

SECURITY CATEGORY

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
Control Environment			
CC1.1 COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
CC1.1	The organization has established procedures for staff to acknowledge applicable company policies periodically.	Inspected employee acknowledgment records to verify that personnel had periodically acknowledged applicable company policies. Confirmed that acknowledgments were completed in a timely manner and in accordance with the organization's defined procedures during the audit period.	No exceptions noted.
CC1.1	The organization has established procedures for new staff to acknowledge applicable company policies as part of their onboarding.	Inspected the Human Resource Policy to determine that all staff acknowledge the applicable security policies during onboarding and annually thereafter. Inquired with the organization and noted that no new staff were onboarded during the audit period.	No exceptions noted.
CC1.1	The organization has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the organization's documented Acceptable Use Policy to confirm that it defines behavioral standards and acceptable business conduct. Verified that the policy was approved, current, and made available to personnel during the audit period.	No exceptions noted.
CC1.1	The organization outlines and documents cybersecurity responsibilities for all personnel.	Inspected the organizational chart and Information security policy to determine that the organization outlines and documents cybersecurity responsibilities for all personnel.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC1.2 COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
CC1.2	The organization's Senior Management reviews and approves all company policies annually.	Inspected key policies of the organization and noted that each was reviewed and approved by Senior Management during the audit period. The review dates and approver details were clearly recorded.	No exceptions noted.
CC1.2	The organization's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the organization's current organizational chart, which included evidence of annual review and approval by senior management, to verify that the chart is reviewed and approved on an annual basis.	No exceptions noted.
CC1.2	The organization's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Management Matrix and Policy to determine that risk assessments are performed annually with quarterly reviews, and remediation activities must be tracked through the ticketing system.	No exceptions noted.
CC1.2	The organization's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information Security policy document to verify that it includes the Information Security program and that it has been reviewed and approved by Senior Management at the defined review frequency. Confirmed the presence of version history, review dates, and documented approval.	No exceptions noted.
CC1.2	The organization's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the organization's Vendor Risk Assessment and verified that it was reviewed and approved by the management during the audit period. The report included identification and risk ratings of relevant vendors and was approved as part of the	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		organization's annual risk assessment process.	
CC1.3 COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
CC1.3	The organization has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Inspected the organization's asset management policy to confirm it defines ownership and protection responsibilities. Also, Inspected the asset inventory list to verify assignment of devices. Inquired with the founder to confirm no assets were added or removed during the audit period and that asset ownership responsibilities are understood and followed.	No exceptions noted.
CC1.3	The organization has established procedures to communicate with staff about their roles and responsibilities.	Inspected the Job Descriptions for a sample of job roles to determine that the organization has established procedures to communicate with staff about their roles and responsibilities.	No exceptions noted.
CC1.3	The organization maintains an organizational structure to define authorities, facilitate information flow and establish responsibilities.	Inspected the organization's documented organizational chart to confirm it defines roles, reporting lines, and areas of responsibility. Verified that the structure is current and reflects key functions and reporting relationships necessary to support authority, communication, and responsibility across the organization.	No exceptions noted.
CC1.3	The organization appoints a Compliance Program Manager who is delegated the responsibility of planning and implementing the internal control environment.	Inspected the organization's org chart and confirmed through inquiry with management that the Compliance Program Manager role has been formally assigned to executive leadership to oversee planning and implementation of the internal control environment.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC1.3	The organization's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the client's Information Security Policy to determine that the organization's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC1.3	The organization's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information Security policy document to verify that it includes the Information Security program and that it has been reviewed and approved by Senior Management at the defined review frequency. Confirmed the presence of version history, review dates, and documented approval.	No exceptions noted.
CC1.3	The organization appoints a People Operations Officer to develop and drive all personnel-related security strategies.	Inspected the organizational structure to verify that executive leadership is responsible for overseeing personnel-related security and compliance activities. Reviewed role assignments to confirm that these responsibilities are managed under executive supervision.	No exceptions noted.
CC1.4 COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			
CC1.4	The organization has established procedures to perform security risk screening of individuals before authorizing access.	Inspected documented policies and procedures related to security risk screening and inquired with management to confirm that such screening is performed prior to authorizing access to organizational systems.	No exceptions noted.
CC1.4	The organization has procedures to ensure that all security-related positions are	Inspected HR policies and sampled personnel files to verify that individuals in	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	staffed by qualified individuals who have the necessary skill set.	security-related roles possessed the required qualifications and skills.	
CC1.5 COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			
CC1.5	The organization has established procedures for staff to acknowledge applicable company policies periodically.	Inspected employee acknowledgment records to verify that personnel had periodically acknowledged applicable company policies. Confirmed that acknowledgments were completed in a timely manner and in accordance with the organization's defined procedures during the audit period.	No exceptions noted.
CC1.5	The organization provides information security and privacy training to staff that is relevant to their job function.	Inspected the Training Dashboard and also Inspected Security Awareness & Training Policy to determine that the personnel complete role-based security training during onboarding and annual refreshers to align with security and operational criteria.	No exceptions noted.
CC1.5	The organization requires that all employees in client serving, IT, Engineering, and Information Security roles are periodically evaluated regarding their job responsibilities.	Inspected policies and a sample of performance evaluation records to verify that employees in client-serving, IT, Engineering, and Information Security roles were periodically evaluated against their job responsibilities.	No exceptions noted.
CC1.5	The organization has established procedures for new staff to complete security and privacy literacy training as part of their onboarding.	Inspected training policies and obtained evidence of completed security and privacy training records to verify that all staff are required to complete such training as part of the onboarding process.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC1.5	The organization documents, monitors, and retains individual training activities and records.	Inspected the Corporate Information Assurance & Governance Policy to determine that the management shall monitor training completion and shall take appropriate steps to ensure compliance with this policy. Also, Inspected the training dashboard in the compliance monitoring platform to determine that the organization provides information security and privacy training to staff that is relevant to their job function.	No exceptions noted.
Information and Communication			
CC2.1 COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
CC2.1	The organization has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the organization's Data Classification, Retention, and Deletion Policy which includes documented guidelines for retaining and securely disposing of information based on data type. Confirmed that the policy was documented, approved by management, and current during the audit period.	No exceptions noted.
CC2.1	The organization displays the most current information about its services on its website, which is accessible to its customers.	Inspected the organization's publicly available website and verified that accurate and current information about its services is presented and readily accessible to customers.	No exceptions noted.
CC2.1	The organization makes all policies and procedures available to all staff members for their perusal.	Inspected that all policies and procedures are stored in a centralized and accessible location. All documentation is readily available for reference by the responsible person to	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		all staff members for their perusal.	
CC2.1	The organization has documented policy and procedures for physical and/or logical labeling of information via documented policy for data classification.	Inspected the organization's Data Classification Policy and confirmed it defines levels of classification and handling procedures for both physical and logical information. Verified that the founder applies these classifications when managing system documentation and customer data.	No exceptions noted.
CC2.1	The organization's systems generate information that is reviewed and evaluated to determine impacts on the functioning of internal controls.	Inspected system-generated alerts and log records to confirm that operational and security events are captured in real time. Verified that these records are reviewed by designated personnel to assess potential impacts on the functioning of internal controls.	No exceptions noted.
CC2.2 COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
CC2.2	The organization has established procedures for staff to acknowledge applicable company policies periodically.	Inspected employee acknowledgment records to verify that personnel had periodically acknowledged applicable company policies. Confirmed that acknowledgments were completed in a timely manner and in accordance with the organization's defined procedures during the audit period.	No exceptions noted.
CC2.2	The organization has established procedures for new staff to acknowledge applicable company policies as part of their onboarding.	Inspected the Human Resource Policy to determine that all staff acknowledge the applicable security policies during onboarding and annually thereafter. Inquired with the organization and noted that no new staff	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		were onboarded during the audit period.	
CC2.2	The organization has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the organization in the event there are problems.	Inspected the organization's Incident Response policies and procedures to verify that they include guidance for employees on reporting incidents, failures, or concerns related to the organization's services or systems. Confirmed that the procedures were made available to personnel and included appropriate reporting channels.	No exceptions noted.
CC2.2	The organization makes all policies and procedures available to all staff members for their perusal.	Inspected that all policies and procedures are stored in a centralized and accessible location. All documentation is readily available for reference by the responsible person to all staff members for their perusal.	No exceptions noted.
CC2.2	The organization has a documented policy to define behavioral standards and acceptable business conduct.	Inspected the organization's documented Acceptable Use Policy to confirm that it defines behavioral standards and acceptable business conduct. Verified that the policy was approved, current, and made available to personnel during the audit period.	No exceptions noted.
CC2.2	The organization has established procedures for new staff to complete security and privacy literacy training as part of their onboarding.	Inspected training policies and obtained evidence of completed security and privacy training records to verify that all staff are required to complete such training as part of the onboarding process.	No exceptions noted.
CC2.2	The organization documents, monitors, and retains individual training activities and records.	Inspected the Corporate Information Assurance & Governance Policy to determine that the management shall monitor training completion and shall	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		take appropriate steps to ensure compliance with this policy. Also, Inspected the training dashboard in the compliance monitoring platform to determine that the organization provides information security and privacy training to staff that is relevant to their job function.	
CC2.3 COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
CC2.3	The organization displays the most current information about its services on its website, which is accessible to its customers.	Inspected the organization's publicly available website and verified that accurate and current information about its services is presented and readily accessible to customers.	No exceptions noted.
CC2.3	The organization has provided information to customers on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the organization in the event there are problems.	Inspected the organization's public-facing website and observed that a Contact Us page and support email option are available, providing customers with a clear and accessible means to report failures, incidents, concerns, or complaints related to the services.	No exceptions noted.
Risk Assessment			
CC3.1 COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
CC3.1	The organization performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the organization's risk assessment documentation and noted that a formal risk assessment was performed within the audit period in accordance with the organization's documented procedures. The assessment identified potential threats to the system's security commitments and included	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		appropriate management review.	
CC3.2 COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
CC3.2	The organization has established procedures for new staff to acknowledge applicable company policies as part of their onboarding.	Inspected the Human Resource Policy to determine that all staff acknowledge the applicable security policies during onboarding and annually thereafter. Inquired with the organization and noted that no new staff were onboarded during the audit period.	No exceptions noted.
CC3.2	The organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor's inventory to determine that the organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC3.2	The organization performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the organization's risk assessment documentation and noted that a formal risk assessment was performed within the audit period in accordance with the organization's documented procedures. The assessment identified potential threats to the system's security commitments and included appropriate management review.	No exceptions noted.
CC3.2	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors	Inspected the organization's risk assessment documentation and confirmed that each identified risk was evaluated using a structured scoring method based on likelihood and impact. The risk assessment considered potential effects on the	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	that address some or all of the risk.	security, availability, and confidentiality of the platform. Each risk was mapped to corresponding mitigating controls or measures.	
CC3.3 COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
CC3.3	The organization considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	Inspected the Risk Register to determine that the organization considers the potential for fraud when assessing risks. This is an entry in the risk matrix.	No exceptions noted.
CC3.4 COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
CC3.4	The organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor's inventory to determine that the organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC3.4	The organization performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the organization's risk assessment documentation and noted that a formal risk assessment was performed within the audit period in accordance with the organization's documented procedures. The assessment identified potential threats to the system's security commitments and included appropriate management review.	No exceptions noted.
CC3.4	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors	Inspected the organization's risk assessment documentation and confirmed that each identified risk was evaluated using a structured scoring method based on likelihood and impact. The risk assessment considered	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	that address some or all of the risk.	potential effects on the security, availability, and confidentiality of the platform. Each risk was mapped to corresponding mitigating controls or measures.	
Monitoring Activities			
CC4.1 COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
CC4.1	The organization has set up mechanisms to assign and manage asset ownership responsibilities and establish a common understanding of asset protection requirements.	Inspected the organization's asset management policy to confirm it defines ownership and protection responsibilities. Also, Inspected the asset inventory list to verify assignment of devices. Inquired with the founder to confirm no assets were added or removed during the audit period and that asset ownership responsibilities are understood and followed.	No exceptions noted.
CC4.1	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected evidence from the automated compliance monitoring platform, a continuous monitoring system and confirmed that it actively tracks the health of the information security program. Regular reports and dashboards are generated and shared with Senior Management and other stakeholders for ongoing oversight.	No exceptions noted.
CC4.1	The organization's Senior Management reviews and approves all company policies annually.	Inspected key policies of the organization and noted that each was reviewed and approved by Senior Management during the audit period. The review dates and approver details were clearly recorded.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC4.1	The organization's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the organization's current organizational chart, which included evidence of annual review and approval by senior management, to verify that the chart is reviewed and approved on an annual basis.	No exceptions noted.
CC4.1	The organization's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Management Matrix and Policy to determine that risk assessments are performed annually with quarterly reviews, and remediation activities must be tracked through the ticketing system.	No exceptions noted.
CC4.1	The organization's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	Inspected the client's Information Security Policy to determine that the organization's Senior Management assigns the role of Information Security Officer who is delegated to centrally manage, coordinate, develop, implement, and maintain an enterprise-wide cybersecurity and privacy program.	No exceptions noted.
CC4.1	The organization's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information Security policy document to verify that it includes the Information Security program and that it has been reviewed and approved by Senior Management at the defined review frequency. Confirmed the presence of version history, review dates, and documented approval.	No exceptions noted.
CC4.1	The organization's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the organization's Vendor Risk Assessment and verified that it was reviewed and approved by the management during the audit period. The report included identification and risk ratings of relevant vendors and was approved as part of the	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		organization's annual risk assessment process.	
CC4.1	The organization reviews and evaluates all subservice organizations periodically, to ensure commitments to the organization's customers can be met.	Inspected documentation for subservice organization oversight and noted that periodic evaluations were conducted to assess their performance and alignment with customer-related commitments. Evidence included vendor reviews and third-party assurance reports.	No exceptions noted.
CC4.1	The organization periodically updates and reviews the inventory of systems as part of installations, removals, and system updates.	Inspected system inventory dashboards to verify that records of active devices are maintained and periodically updated during installations, removals, and system updates.	No exceptions noted.
CC4.2 COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
CC4.2	The organization has provided information to employees, via various Information Security Policies/procedures, on how to report failures, incidents, concerns, or other complaints related to the services or systems provided by the organization in the event there are problems.	Inspected the organization's Incident Response policies and procedures to verify that they include guidance for employees on reporting incidents, failures, or concerns related to the organization's services or systems. Confirmed that the procedures were made available to personnel and included appropriate reporting channels.	No exceptions noted.
CC4.2	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected evidence from the automated compliance monitoring platform, a continuous monitoring system and confirmed that it actively tracks the health of the information security program. Regular reports and dashboards are generated and shared with Senior Management and other	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		stakeholders for ongoing oversight.	
CC4.2	The organization's Senior Management reviews and approves all company policies annually.	Inspected key policies of the organization and noted that each was reviewed and approved by Senior Management during the audit period. The review dates and approver details were clearly recorded.	No exceptions noted.
CC4.2	The organization's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information Security policy document to verify that it includes the Information Security program and that it has been reviewed and approved by Senior Management at the defined review frequency. Confirmed the presence of version history, review dates, and documented approval.	No exceptions noted.
Control Activities			
CC5.1 COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			
CC5.1	The organization has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.	Inspected the organization's documented policies and procedures to confirm that they define expected behavior in alignment with the organization's control environment. Verified that the documents cover ethical conduct, accountability, management tone, and other behavioral expectations. Also verified that these were communicated to personnel and approved by senior management.	No exceptions noted.
CC5.1	The organization's Senior Management segregates responsibilities and duties across the organization to mitigate risks to the services provided to its customers.	Inspected the organizational chart and access control matrix to verify that roles and responsibilities are segregated among personnel. Confirmed that the segregation of duties	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		is designed to reduce the risk of conflicts and unauthorized activities.	
CC5.1	The organization establishes guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	Inspected the Acceptable Use Policy to determine that the organization has established guidelines for acceptable and unacceptable technology usage behaviors, including outlining consequences for unacceptable actions.	No exceptions noted.
CC5.2 COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
CC5.2	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected evidence from the automated compliance monitoring platform, a continuous monitoring system and confirmed that it actively tracks the health of the information security program. Regular reports and dashboards are generated and shared with Senior Management and other stakeholders for ongoing oversight.	No exceptions noted.
CC5.2	The organization has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.	Inspected the organization's documented policies and procedures to confirm that they define expected behavior in alignment with the organization's control environment. Verified that the documents cover ethical conduct, accountability, management tone, and other behavioral expectations. Also verified that these were communicated to personnel and approved by senior management.	No exceptions noted.
CC5.2	The organization's Senior Management reviews and approves all company policies annually.	Inspected key policies of the organization and noted that each was reviewed and approved by Senior Management during the audit	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		period. The review dates and approver details were clearly recorded.	
CC5.2	The organization's Senior Management reviews and approves the Organizational Chart for all employees annually.	Inspected the organization's current organizational chart, which included evidence of annual review and approval by senior management, to verify that the chart is reviewed and approved on an annual basis.	No exceptions noted.
CC5.2	The organization's Senior Management reviews and approves the "Risk Assessment Report" annually.	Inspected the Risk Management Matrix and Policy to determine that risk assessments are performed annually with quarterly reviews, and remediation activities must be tracked through the ticketing system.	No exceptions noted.
CC5.2	The organization's Senior Management reviews and approves the state of the Information Security program including policies, standards, and procedures, at planned intervals or if significant changes occur to ensure their continuing suitability, adequacy, and effectiveness.	Inspected the Information Security policy document to verify that it includes the Information Security program and that it has been reviewed and approved by Senior Management at the defined review frequency. Confirmed the presence of version history, review dates, and documented approval.	No exceptions noted.
CC5.2	The organization's Senior Management reviews and approves the "Vendor Risk Assessment Report" annually.	Inspected the organization's Vendor Risk Assessment and verified that it was reviewed and approved by the management during the audit period. The report included identification and risk ratings of relevant vendors and was approved as part of the organization's annual risk assessment process.	No exceptions noted.
CC5.2	The organization reviews and evaluates all subservice organizations periodically, to ensure commitments to the organization's customers can be met.	Inspected documentation for subservice organization oversight and noted that periodic evaluations were conducted to assess their performance and alignment	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		with customer-related commitments. Evidence included vendor reviews and third-party assurance reports.	
CC5.3 COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
CC5.3	The organization has established procedures for staff to acknowledge applicable company policies periodically.	Inspected employee acknowledgment records to verify that personnel had periodically acknowledged applicable company policies. Confirmed that acknowledgments were completed in a timely manner and in accordance with the organization's defined procedures during the audit period.	No exceptions noted.
CC5.3	The organization has established procedures for new staff to acknowledge applicable company policies as part of their onboarding.	Inspected the Human Resource Policy to determine that all staff acknowledge the applicable security policies during onboarding and annually thereafter. Inquired with the organization and noted that no new staff were onboarded during the audit period.	No exceptions noted.
CC5.3	The organization has documented a set of policies and procedures that establish expected behavior with regard to the Company's control environment.	Inspected the organization's documented policies and procedures to confirm that they define expected behavior in alignment with the organization's control environment. Verified that the documents cover ethical conduct, accountability, management tone, and other behavioral expectations. Also verified that these were communicated to personnel and approved by senior management.	No exceptions noted.
CC5.3	The organization makes all policies and procedures	Inspected that all policies and procedures are stored in a centralized and accessible	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	available to all staff members for their perusal.	location. All documentation is readily available for reference by the responsible person to all staff members for their perusal.	
Logical and Physical Controls			
CC6.1 The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.			
CC6.1	The organization ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected access records and system logs, the service auditor found that access to critical systems was provisioned by the authorized individual in accordance with the organization's role-based access policy.	No exceptions noted.
CC6.1	The organization has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the organization's access control policies and procedures and inspected the user provisioning process to verify that new users are registered, authorized, and granted system credentials only upon approval for accessing critical systems.	No exceptions noted.
CC6.1	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to alert the security team to update the access levels of team members whose roles have changed.	Inspected the automated compliance monitoring platform configuration and confirmed that it is set to alert on role changes requiring access updates whose roles have changed. No role changes occurred during the audit period.	No exceptions noted.
CC6.1	The organization ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected network and system configuration settings and reviewed supporting evidence to verify that production database access and Secure Shell (SSH) access to infrastructure entities are restricted from public internet access.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC6.1	The organization's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected evidence of periodic access reviews performed by Senior Management or the Information Security Officer to verify that access to critical systems is limited to individuals with a valid business need.	No exceptions noted.
CC6.1	The organization's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected the administrative access review spreadsheet, which lists users with administrative privileges, their roles, and associated critical systems, along with the review date and reviewer details, to confirm that administrative access is restricted to individuals requiring such access to perform their job functions.	No exceptions noted.
CC6.1	The organization has documented guidelines to manage passwords and secure login mechanisms and makes them available to all staff members on the company employee portal.	Inspected the organization's documented password and login policy and verified that it is accessible to all employees. Also reviewed endpoint configurations to confirm alignment with the defined security practices.	No exceptions noted.
CC6.1	The organization has documented policies and procedures to manage physical and environmental security.	Inspected the organization's documented policies and procedures related to physical and environmental security to confirm that requirements for facility access, asset protection, and environmental safeguards are formally defined and maintained.	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.			
CC6.2	The organization ensures that logical access provisioning to critical systems requires approval from authorized	Inspected access records and system logs, the service auditor found that access to critical systems was	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	personnel on an individual need or for a predefined role.	provisioned by the authorized individual in accordance with the organization's role-based access policy.	
CC6.2	The organization has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the organization's access control policies and procedures and inspected the user provisioning process to verify that new users are registered, authorized, and granted system credentials only upon approval for accessing critical systems.	No exceptions noted.
CC6.2	The organization ensures logical access that is no longer required in the event of termination is made inaccessible in a timely manner.	Inspected the organization's Access Management Policy and related procedures outlining the de-provisioning of logical access when no longer required. This included processes for revoking access granted to third-party services and integrations.	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.			
CC6.3	The organization ensures that logical access provisioning to critical systems requires approval from authorized personnel on an individual need or for a predefined role.	Inspected access records and system logs, the service auditor found that access to critical systems was provisioned by the authorized individual in accordance with the organization's role-based access policy.	No exceptions noted.
CC6.3	The organization has documented policies and procedures to manage Access Control and an accompanying process to register and authorize users for issuing system credentials which grant the ability to access the critical systems.	Inspected the organization's access control policies and procedures and inspected the user provisioning process to verify that new users are registered, authorized, and granted system credentials only upon approval for accessing critical systems.	No exceptions noted.
CC6.3	The organization ensures logical access that is no	Inspected the organization's Access Management Policy	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	longer required in the event of termination is made inaccessible in a timely manner.	and related procedures outlining the de-provisioning of logical access when no longer required. This included processes for revoking access granted to third-party services and integrations. No terminations were made during the audit window.	
CC6.3	The organization's Senior Management or the Information Security Officer periodically reviews and ensures that access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected evidence of periodic access reviews performed by Senior Management or the Information Security Officer to verify that access to critical systems is limited to individuals with a valid business need.	No exceptions noted.
CC6.3	The organization ensures that access to the production databases is restricted to only those individuals who require such access to perform their job functions.	Inspected database access control lists and user permission settings to verify that only authorized individuals with a business need have access to production databases; reviewed role-based access assignments and inquired with management to confirm appropriateness of access.	No exceptions noted.
CC6.3	The organization's Senior Management or the Information Security Officer periodically reviews and ensures that administrative access to the critical systems is restricted to only those individuals who require such access to perform their job functions.	Inspected the administrative access review spreadsheet, which lists users with administrative privileges, their roles, and associated critical systems, along with the review date and reviewer details, to confirm that administrative access is restricted to individuals requiring such access to perform their job functions.	No exceptions noted.
CC6.4 The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
CC6.4	The organization maintains documented building and	Inspected the building and workplace security document	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	workplace rules, including opening hours, entry procedures, visitor handling requirements, and emergency information (fire exits, alarms), and ensures this information is communicated by building management.	confirming controlled entry procedures, operating hours, emergency protocols, and restricted access to the client office. Verified that these practices were in place and followed during the audit period.	
CC6.4	The organization maintains and reviews access to the office premises through a smart-lock or key register, ensures timely revocation for leavers, and performs periodic door access log reviews to detect unauthorized access.	Inspected the office key and equipment assignment log to confirm that physical access to restricted areas is controlled, assigned only to authorized personnel, and periodically updated. Verified that issuance and return dates demonstrate operation of this control during the audit period.	No exceptions noted.
CC6.4	The organization enforces visitor control procedures, including maintaining a visitor log or documenting a “no visitors” environment, issuing visitor badges or stickers, and ensuring that all visitors are escorted within the premises.	Inspected the organization’s documented statement confirming that visitors are not permitted within the office premises due to privacy and NDA requirements, and verified that this policy operated during the audit period.	No exceptions noted.
CC6.4	The organization ensures secure physical storage of sensitive assets by maintaining locked cabinets, managing key-holder assignments, and documenting the shredding or secure disposal of sensitive documents.	Inspected evidence of the organization’s locked storage cabinets and the corresponding key-holder list to confirm that sensitive physical assets are stored in secured cabinets accessible only to authorized personnel. Verified that this practice operated during the audit period.	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.			
CC6.5	The organization has a documented policy that provides guidance on decommissioning of	Inspected the organization’s Data Classification, Retention, and Deletion Policy and confirmed that it provides	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	information assets that contain classified information.	guidance for securely disposing of information assets containing classified data. The policy includes approved disposal methods and documentation requirements. Verified that the policy was reviewed during the audit period.	
CC6.6 The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
CC6.6	Where applicable, the organization ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected device compliance dashboards and reviewed endpoint security policies to confirm that disk encryption is enabled on systems accessing critical data to protect against unauthorized access or data exposure.	No exceptions noted.
CC6.6	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the organization's cloud provider.	Inspected firewall and network security configurations and reviewed supporting evidence to verify that production hosts are protected by firewall rules configured with a deny-by-default posture.	No exceptions noted.
CC6.6	The organization requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected centralized device compliance dashboards and reviewed endpoint configuration policies to confirm that disk encryption is enforced and monitored on all critical endpoints to protect against unauthorized access.	No exceptions noted.
CC6.6	The organization ensures that the production databases access and Secure Shell access to infrastructure entities are protected from public internet access.	Inspected network and system configuration settings and reviewed supporting evidence to verify that production database access and Secure Shell (SSH) access to infrastructure entities are restricted from public internet access.	No exceptions noted.
CC6.6	Where applicable, the organization ensures that	Inspected device compliance dashboards and reviewed	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	endpoints with access to critical servers or data must be protected by malware-protection software.	endpoint security configurations to confirm that malware-protection software is installed and monitored on systems accessing critical data to safeguard against malicious threats.	
CC6.6	The organization has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inspected device compliance dashboard and reviewed detailed security configuration checks to confirm that all remote devices undergo periodic compliance verification before accessing internal systems or organizational resources.	No exceptions noted.
CC6.6	The organization ensures that endpoints with access to critical servers or data are configured to automatically lock after a period of inactivity.	Inspected device compliance dashboards and reviewed endpoint configuration policies to confirm that systems accessing critical data are set to automatically lock after a defined period of inactivity and require password re-authentication for access.	No exceptions noted.
CC6.6	The organization has documented guidelines to manage communications protections and network security of critical systems.	Inspected the organization's Encryption and Key Usage Policy for communication protections and network security. Confirmed that the guidelines include use of secure protocols i.e., HTTPS, TLS and restricted access to critical systems.	No exceptions noted.
CC6.6	The organization requires that all staff members with access to any critical system be protected with a secure login mechanism such as Multifactor-authentication.	Inspected organizational security settings and verified that 2-Step Verification is enforced at the domain level, requiring staff with access to critical systems to authenticate using multifactor methods such as verification codes or security keys in addition to their passwords.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC6.6	The organization has documented policies and procedures for endpoint security and related controls.	Inspected the organization's documented policies and procedures to confirm that requirements related to endpoint security are formally defined, maintained, and approved by management.	No exceptions noted.
CC6.6	The organization develops, documents, and maintains an inventory of organizational endpoint systems, including all necessary information to achieve accountability.	Inspected the organization's asset inventory and reviewed endpoint configuration to confirm that all organizational systems are documented, assigned to responsible users, and tracked to ensure accountability.	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.			
CC6.7	Where applicable, the organization ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected device compliance dashboards and reviewed endpoint security policies to confirm that disk encryption is enabled on systems accessing critical data to protect against unauthorized access or data exposure.	No exceptions noted.
CC6.7	The organization has set up cryptographic mechanisms to encrypt all production databases that store customer data at rest.	Inspected system configuration settings and supporting documentation to verify that cryptographic mechanisms are implemented to encrypt production databases containing customer data at rest.	No exceptions noted.
CC6.7	The organization requires that all critical endpoints are encrypted to protect them from unauthorized access.	Inspected centralized device compliance dashboards and reviewed endpoint configuration policies to confirm that disk encryption is enforced and monitored on all critical endpoints to protect against unauthorized access.	No exceptions noted.
CC6.7	The organization has set up processes to utilize standard encryption methods, including	Inspected the TLS certificate applied to the organization's public-facing domain and	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	HTTPS with the TLS algorithm, to keep transmitted data confidential.	confirmed that the site enforces secure transmission using HTTPS to keep transmitted data confidential.	
CC6.7	The organization has a documented policy to manage encryption and cryptographic protection controls.	Inspected the Encryption & Cryptographic Control Policy to determine that the organization has a documented policy to manage encryption and cryptographic protection controls.	No exceptions noted.
CC6.7	The organization develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Inspected the organization's documented infrastructure inventory and verified that it includes relevant systems and associated details necessary to achieve accountability. Additionally, inquired with management to confirm that the inventory is maintained and updated on an ongoing basis.	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.			
CC6.8	Every Production host is protected by a firewall with a deny-by-default rule. Deny by default rule set is a default on the organization's cloud provider.	Inspected firewall and network security configurations and reviewed supporting evidence to verify that production hosts are protected by firewall rules configured with a deny-by-default posture.	No exceptions noted.
CC6.8	The organization has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inspected device compliance dashboard and reviewed detailed security configuration checks to confirm that all remote devices undergo periodic compliance verification before accessing internal systems or organizational resources.	No exceptions noted.
System Operations			
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.			

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC7.1	The organization has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inspected system monitoring configurations and supporting documentation to verify that critical assets are continuously monitored and capacity alerts are configured to support performance management and availability.	No exceptions noted.
CC7.1	The organization identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected vulnerability management documentation and reviewed evidence of vulnerability scanning activities to verify that the organization performs regular vulnerability scans on the Company platform.	No exceptions noted.
CC7.1	The organization's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected logging and audit configuration settings and reviewed supporting documentation to verify that audit events are generated for security-relevant actions on critical systems.	No exceptions noted.
CC7.1	The organization tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected the organization’s vulnerability management policy and reviewed supporting evidence to verify that identified vulnerabilities are tracked and remediated in accordance with defined policies and procedures.	No exceptions noted.
CC7.1	The organization's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Inspected logging and monitoring configurations and reviewed supporting documentation to verify that audit events are configured to be reviewed and analyzed for the detection of anomalous or suspicious activity and threats.	No exceptions noted.
CC7.1	The organization has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inspected the organization's documented Vulnerability Management Policy and procedures to confirm that they outline responsibilities, timelines, and processes for identifying, assessing, and remediating technical vulnerabilities.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC7.2 The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.			
CC7.2	The organization has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inspected system monitoring configurations and supporting documentation to verify that critical assets are continuously monitored and capacity alerts are configured to support performance management and availability.	No exceptions noted.
CC7.2	The organization identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected vulnerability management documentation and reviewed evidence of vulnerability scanning activities to verify that the organization performs regular vulnerability scans on the Company platform.	No exceptions noted.
CC7.2	The organization's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected logging and audit configuration settings and reviewed supporting documentation to verify that audit events are generated for security-relevant actions on critical systems.	No exceptions noted.
CC7.2	The organization tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected the organization’s vulnerability management policy and reviewed supporting evidence to verify that identified vulnerabilities are tracked and remediated in accordance with defined policies and procedures.	No exceptions noted.
CC7.2	The organization's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Inspected logging and monitoring configurations and reviewed supporting documentation to verify that audit events are configured to be reviewed and analyzed for the detection of anomalous or suspicious activity and threats.	No exceptions noted.
CC7.2	The organization has a documented policy and procedures to establish	Inspected the organization's documented Vulnerability Management Policy and procedures to confirm that	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	guidelines for managing technical vulnerabilities.	they outline responsibilities, timelines, and processes for identifying, assessing, and remediating technical vulnerabilities.	
CC7.3 The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.			
CC7.3	The organization has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inspected system monitoring configurations and supporting documentation to verify that critical assets are continuously monitored and capacity alerts are configured to support performance management and availability.	No exceptions noted.
CC7.3	The organization has documented guidelines on notifying customers and other stakeholders in case of a breach.	Inspected the organization's incident response policy and confirmed that it includes documented guidelines for notifying customers and stakeholders in the event of a breach. The policy outlines roles, timelines, and communication methods. Additionally, inspected the organization's website, including the blogs and updates section, and noted that it may be used as a channel for communicating important updates or incidents.	No exceptions noted.
CC7.3	The organization maintains a record of information security incidents, their investigations, and the response plans that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the organization's incident response and handling policy to determine that the organization maintains a record of information security incidents, their investigations, and the response plans that was executed in accordance with the policy and procedure defined to report and manage incidents.	Not tested. No security incident occurred during the audit period.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC7.3	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to track and report the health of the information security program to the Information Security Officer and other stakeholders.	Inspected evidence from the automated compliance monitoring platform, a continuous monitoring system and confirmed that it actively tracks the health of the information security program. Regular reports and dashboards are generated and shared with Senior Management and other stakeholders for ongoing oversight.	No exceptions noted.
CC7.3	The organization identifies vulnerabilities on the Company platform through the execution of regular vulnerability scans.	Inspected vulnerability management documentation and reviewed evidence of vulnerability scanning activities to verify that the organization performs regular vulnerability scans on the Company platform.	No exceptions noted.
CC7.3	The organization has set up measures to perform security and privacy compliance checks on the software versions and patches of remote devices prior to the establishment of the internal connection.	Inspected device compliance dashboard and reviewed detailed security configuration checks to confirm that all remote devices undergo periodic compliance verification before accessing internal systems or organizational resources.	No exceptions noted.
CC7.3	The organization's infrastructure is configured to generate audit events for actions of interest related to security for all critical systems.	Inspected logging and audit configuration settings and reviewed supporting documentation to verify that audit events are generated for security-relevant actions on critical systems.	No exceptions noted.
CC7.3	The organization tracks all vulnerabilities and remediates them as per the policy and procedure defined to manage vulnerabilities.	Inspected the organization’s vulnerability management policy and reviewed supporting evidence to verify that identified vulnerabilities are tracked and remediated in accordance with defined policies and procedures.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC7.3	The organization's infrastructure is configured to review and analyze audit events to detect anomalous or suspicious activity and threats.	Inspected logging and monitoring configurations and reviewed supporting documentation to verify that audit events are configured to be reviewed and analyzed for the detection of anomalous or suspicious activity and threats.	No exceptions noted.
CC7.3	The organization identifies vulnerabilities on the company platform through an annual penetration testing exercise conducted by a qualified third-party service provider.	Inspected penetration testing documentation and reviewed supporting evidence to verify that an annual penetration test was conducted on the Company platform by a qualified third-party service provider.	No exceptions noted.
CC7.3	The organization has a documented policy and procedures to establish guidelines for managing technical vulnerabilities.	Inspected the organization's documented Vulnerability Management Policy and procedures to confirm that they outline responsibilities, timelines, and processes for identifying, assessing, and remediating technical vulnerabilities.	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.			
CC7.4	The organization maintains a record of information security incidents, their investigations, and the response plans that was executed in accordance with the policy and procedure defined to report and manage incidents.	Inspected the organization's incident response and handling policy to determine that the organization maintains a record of information security incidents, their investigations, and the response plans that was executed in accordance with the policy and procedure defined to report and manage incidents.	Not tested. No security incident occurred during the audit period.
CC7.4	The organization uses an automated compliance monitoring platform, a continuous monitoring system, to track and report the health of the information	Inspected evidence from the automated compliance monitoring platform, a continuous monitoring system and confirmed that it actively tracks the health of the	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	security program to the Information Security Officer and other stakeholders.	information security program. Regular reports and dashboards are generated and shared with Senior Management and other stakeholders for ongoing oversight.	
CC7.4	The organization has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	Inspected the organization's incident response and handling policy to determine that the organization has established a policy and procedure which includes guidelines to be undertaken in response to information security incidents.	No exceptions noted.
CC7.5 The entity identifies, develops, and implements activities to recover from identified security incidents.			
CC7.5	The organization has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the backup and disaster recovery policy and procedures to determine that the organization has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
CC7.5	The organization has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the organization's documented Business Continuity Policy and Disaster Recovery plan to verify that it includes procedures for continuing business operations in the event of a disruption or security incident. Confirmed that the Disaster recovery plan was approved by management, current during the audit period, and included roles, responsibilities, and recovery steps.	No exceptions noted.
CC7.5	The organization has documented policies and procedures that establish guidelines for continuing business operations and	Inspected the organization's Business Continuity and Contingency Planning documentation and confirmed that policies and procedures	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	facilitate the application of contingency planning controls.	are in place to guide continued operations during disruptive events. The plan includes defined roles, recovery strategies, and contingency controls such as data backups and remote access.	
Change Management			
CC8.1 The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
CC8.1	The organization has established procedures for approval when implementing changes to the operating environment.	Inspected the organization's change management policy and reviewed supporting documentation to verify that procedures for approval are established when implementing changes to the operating environment.	No exceptions noted.
CC8.1	The organization has documented policies and procedures to manage changes to its operating environment.	Inspected the organization's change management policy and procedures to verify that they are formally documented, include roles and responsibilities, and outline steps for requesting, reviewing, approving, testing, and implementing changes in the operating environment.	No exceptions noted.
CC8.1	The organization has procedures to govern changes to its operating environment.	Inspected the organization's documented change management procedures and reviewed supporting documentation to verify that procedures are established to govern changes to the operating environment.	No exceptions noted.
CC8.1	The organization develops, documents, and maintains an inventory of organizational infrastructure systems, including all necessary information to achieve accountability.	Inspected the organization's documented infrastructure inventory and verified that it includes relevant systems and associated details necessary to achieve accountability. Additionally, inquired with management to confirm that	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		the inventory is maintained and updated on an ongoing basis.	
Risk Mitigation			
CC9.1 The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
CC9.1	The organization performs a formal risk assessment exercise annually, as per documented guidelines and procedures, to identify threats that could impair systems' security commitments and requirements.	Inspected the organization's risk assessment documentation and noted that a formal risk assessment was performed within the audit period in accordance with the organization's documented procedures. The assessment identified potential threats to the system's security commitments and included appropriate management review.	No exceptions noted.
CC9.1	Each risk is assessed and given a risk score in relation to the likelihood of it occurring and the potential impact on the security, availability, and confidentiality of the Company platform. Risks are mapped to mitigating factors that address some or all of the risk.	Inspected the organization's risk assessment documentation and confirmed that each identified risk was evaluated using a structured scoring method based on likelihood and impact. The risk assessment considered potential effects on the security, availability, and confidentiality of the platform. Each risk was mapped to corresponding mitigating controls or measures.	No exceptions noted.
CC9.1	The organization has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the organization's service commitments and system requirements.	Inspected the Risk Management Policy, Policies and Matrix to determine that the organization has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the organization's service commitments and system requirements.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
CC9.2 The entity assesses and manages risks associated with vendors and business partners.			
CC9.2	The organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	Inspected the vendor's inventory to determine that the organization performs a formal vendor risk assessment exercise annually to identify vendors that are critical to the systems' security commitments and requirements.	No exceptions noted.
CC9.2	The organization has a documented policy and procedures to manage Vendors/third-party suppliers and provides guidance to staff on performing a risk assessment of such vendors.	Inspected the Third-Party Risk Management Policy to determine how the organization assesses, monitors, and mitigates risks introduced by vendors and subservice organizations.	No exceptions noted.
CC9.2	The organization has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the organization's service commitments and system requirements.	Inspected the Risk Management Policy, Policies and Matrix to determine that the organization has documented policies and procedures that describe how to identify risks to business objectives and how those risks are assessed and mitigated. The objectives incorporate the organization's service commitments and system requirements.	No exceptions noted.
ADDITIONAL CRITERIA FOR AVAILABILITY			
A1.1 The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.			
A1.1	The organization has set up methods to continuously monitor critical assets to generate capacity alerts to ensure optimal performance, meet future capacity requirements, and protect against denial-of-service attacks.	Inspected system monitoring configurations and supporting documentation to verify that critical assets are continuously monitored and capacity alerts are configured to support performance management and availability.	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
A1.2 The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data back-up processes, and recovery infrastructure to meet its objectives.			
A1.2	The organization has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	Inspected the backup and disaster recovery policy and procedures to determine that the organization has a documented policy on managing Data Backups and makes it available for all relevant staff on the company employee portal.	No exceptions noted.
A1.2	The organization backs up relevant user and system data regularly to meet recovery time and recovery point objectives and verifies the integrity of these backups.	Inspected backup policies and reviewed supporting evidence to verify that relevant user and system data are backed up on a regular basis and that procedures are in place to verify the integrity of backups.	No exceptions noted.
A1.2	The organization tests backup information periodically to verify media reliability and information integrity.	Inspected backup and recovery procedures and reviewed supporting documentation to verify that backup information is periodically tested to confirm media reliability and information integrity.	No exceptions noted.
A1.2	The organization has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the organization's documented Business Continuity Policy and Disaster Recovery plan to verify that it includes procedures for continuing business operations in the event of a disruption or security incident. Confirmed that the Disaster recovery plan was approved by management, current during the audit period, and included roles, responsibilities, and recovery steps.	No exceptions noted.
A1.2	The organization has documented policies and procedures that establish guidelines for continuing	Inspected the organization’s Business Continuity and Contingency Planning documentation and confirmed	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	business operations and facilitate the application of contingency planning controls.	that policies and procedures are in place to guide continued operations during disruptive events. The plan includes defined roles, recovery strategies, and contingency controls such as data backups and remote access.	
A1.3 The entity tests recovery plan procedures supporting system recovery to meet its objectives.			
A1.3	The organization has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	Inspected the tabletop exercise conducted by the organization to determine that the organization has procedures to conduct regular tests and exercises that determine the effectiveness and the readiness to execute the contingency plan.	No exceptions noted.
A1.3	The organization tests backup information periodically to verify media reliability and information integrity.	Inspected backup and recovery procedures and reviewed supporting documentation to verify that backup information is periodically tested to confirm media reliability and information integrity.	No exceptions noted.
A1.3	The organization has documented guidelines to manage Disaster Recovery that establish guidelines and procedures for continuing business operations in case of a disruption or a security incident.	Inspected the organization's documented Business Continuity Policy and Disaster Recovery plan to verify that it includes procedures for continuing business operations in the event of a disruption or security incident. Confirmed that the Disaster recovery plan was approved by management, current during the audit period, and included roles, responsibilities, and recovery steps.	No exceptions noted.
A1.3	The organization has documented policies and procedures that establish guidelines for continuing business operations and	Inspected the organization’s Business Continuity and Contingency Planning documentation and confirmed that policies and procedures	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
	facilitate the application of contingency planning controls.	are in place to guide continued operations during disruptive events. The plan includes defined roles, recovery strategies, and contingency controls such as data backups and remote access.	
ADDITIONAL CRITERIA FOR CONFIDENTIALITY			
C1.1 The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.			
C1.1	The organization has a documented Information Security Policy that governs the confidentiality, integrity, and availability of information systems.	Inspected the organization's Information Security Policy to verify that it is documented and includes provisions for the confidentiality, integrity, and availability of information systems. Confirmed that the policy was reviewed and approved by management and was current during the audit period.	No exceptions noted.
C1.1	The organization performs physical and/or logical labeling of information systems as per the guidelines documented policy defined for data classification.	Inspected the data classification policy and sampled system assets to confirm they were physically and/or logically labeled in accordance with the documented classification guidelines during the audit period.	No exceptions noted.
C1.1	Where applicable, the organization ensures that endpoints with access to critical servers or data must be encrypted to protect from unauthorized access.	Inspected device compliance dashboards and reviewed endpoint security policies to confirm that disk encryption is enabled on systems accessing critical data to protect against unauthorized access or data exposure.	No exceptions noted.
C1.1	The organization has established procedures for staff to acknowledge applicable company policies periodically.	Inspected employee acknowledgment records to verify that personnel had periodically acknowledged applicable company policies. Confirmed that acknowledgments were	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		completed in a timely manner and in accordance with the organization's defined procedures during the audit period.	
C1.1	The organization has established procedures for new staff to acknowledge applicable company policies as part of their onboarding.	Inspected the Human Resource Policy to determine that all staff acknowledge the applicable security policies during onboarding and annually thereafter. Inquired with the organization and noted that no new staff were onboarded during the audit period.	No exceptions noted.
C1.1	The organization has set up cryptographic mechanisms to encrypt all production databases that store customer data at rest.	Inspected system configuration settings and supporting documentation to verify that cryptographic mechanisms are implemented to encrypt production databases containing customer data at rest.	No exceptions noted.
C1.2 The entity disposes of confidential information to meet the entity's objectives related to confidentiality.			
C1.2	The organization has a documented policy that provides guidance on decommissioning of information assets that contain classified information.	Inspected the organization's Data Classification, Retention, and Deletion Policy and confirmed that it provides guidance for securely disposing of information assets containing classified data. The policy includes approved disposal methods and documentation requirements. Verified that the policy was reviewed during the audit period.	No exceptions noted.
C1.2	The organization has a documented policy outlining guidelines for the disposal and retention of information.	Inspected the organization's Data Classification, Retention, and Deletion Policy which includes documented guidelines for retaining and securely disposing of information based on data type. Confirmed that the policy	No exceptions noted.

Trust ID	Control Description	Test Applied by the Service Auditor	Test Results
		was documented, approved by management, and current during the audit period.	