System and Organization Controls (SOC) 2 Type I Report

Report on Management's Description of

Vyro

And the Suitability of Design of Controls Relevant to the Trust Services Criteria for Security Category

As of September 28, 2022

Together with
Independent Service Auditor's Report

Table of Contents

I. Independent Service Auditor's Report

Independent Service Auditor's Report

Vyro Pty Ltd.

Scope

We have examined Vyro Pty Ltd.'s accompanying description of its Vyro (system) titled "Description of Vyro" as of September 28, 2022 (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria)*, (description criteria) and the suitability of the design of controls stated in the description as of September 28, 2022, to provide reasonable assurance that Vyro Pty Ltd.'s service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria)*.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed 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 of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria.
- 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 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. The projection to the future of any conclusions about the suitability of the design 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.

Other Matter

We did not perform any procedures regarding the operating effectiveness of controls stated in the description and, accordingly, do not express an opinion thereon.

Opinion

In our opinion, in all material respects,

a. The description presents Vyro Pty Ltd.'s Vyro (system) that was designed and implemented as of September 28, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of September 28, 2022, to provide reasonable assurance that Vyro Pty Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Restricted Use

This report is intended solely for the information and use of Vyro Pty Ltd., user entities of Vyro Pty Ltd.'s Vyro (system) as of September 28, 2022, business partners of Vyro Pty Ltd. subject to risks arising from interactions with the Vyro (system), practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

JohansonGroup LLP

Colorado Springs, Colorado
October 12, 2022

II. Assertion of Vyro Pty Ltd. Management

Assertion of Vyro Pty Ltd. Management

We have prepared the accompanying description of Vyro Pty Ltd.'s Vyro (system) titled "Description of Vyro as of September 28, 2022" (description) based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (AICPA, Description Criteria),* (description criteria). The description is intended to provide report users with information about the Vyro (system) that may be useful when assessing the risks arising from interactions with Vyro Pty Ltd.'s system, particularly information about system controls that Vyro Pty Ltd. has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).*

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

a. The description presents Vyro Pty Ltd.'s Vyro (system) that was designed and implemented as of September 28, 2022, in accordance with the description criteria.
b. The controls stated in the description were suitably designed as of September 28, 2022, to provide reasonable assurance that Vyro Pty Ltd.'s service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date.

Vyro Pty Ltd. Management
October 12, 2022

III. Description of Vyro

Description of Vyro

COMPANY BACKGROUND

Vyro is a young startup that runs a virtual dealership for electric vehicles. The company is based in Australia and the main arm of its business is to sell vehicles directly to customers (online). Additionally, Vyro has a B2B solution where they white-label or co-brand their virtual dealership and license it as software to vehicle manufacturers and dealerships around the world.

DESCRIPTION OF SERVICES OVERVIEW OR SERVICES PROVIDED

Vyro's main product/service is the sale of electric vehicles directly to customers (online). Additionally, Vyro has a partnership product where they license their software to partners, such as vehicle manufacturers, dealerships, and other types of organizations.

Vyro's platform provides customers with an online way to:

1) Trade in their car
2) Purchase a new electric car
3) Obtain finance from a number of lenders
4) Purchase additional supporting products (or add-ons) such as home chargers, insurance, and more

Example Use Case - Retail Customer:

A customer wishes to purchase an electric vehicle. They visit Vyro and get a valuation for their current car online. Vyro credits this valuation to the customer's account and the customer uses this to purchase a new electric vehicle, along with a home charger. The amount remaining after the trade-in is financed through one of Vyro's panel of lenders.

Example Use Case - White-labelled Platform:

Everything on the Vyro platform can be replicated and white-labeled for partners who license the Vyro software. For example, a vehicle manufacturer can license the Vyro software to create their white-labeled virtual dealership that achieves everything listed above for their customers.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

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

Vyro's commitments to users are communicated through Service Level Agreements (SLAs) or Master Service Agreements (MSAs), Online Privacy Policy, and in the description of the service offering provided online.

Security Commitments

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

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

COMPONENTS OF THE SYSTEM

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.

Infrastructure

Vyro Pty Ltd. maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents the device name, inventory type, description, and owner. To outline the topology of its network, the organization maintains the following network diagram(s).

Hardware	Type	Purpose
AWS Elastic Compute Cloud (EC2)	AWS	Scalable Computing Capacity
AWS Elastic Load Balancers	AWS	Load balance internal and external traffic
Virtual Private Cloud	AWS	Protects the network perimeter and restricts inbound and outbound access
S3 Buckets	AWS	Storage, upload and download

Software

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

System/Application	Operating System	Purpose
GuardDuty	AWS	Security application used for automated intrusion detection (IDS)
Datadog	Datadog	Monitoring application used to provide monitoring, alter, and notification services for Vyro Pty Ltd platform
Typescript	Linux	Primary development language/runtime for applications
PostgreSQL	Linux	Transactional database

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.

Vyro Pty Ltd. has a staff of approximately 5 organized in the following functional areas:

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

- CEO
- CFO
- CTO
- CRO

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.

Data

Data, as defined by Vyro Pty Ltd, constitutes the following:

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

Data is categorized into the following major types of data used by Vyro Pty Ltd.

Category	Description	Examples
Public	Public information is not confidential and can be made public without any implications for Vyro Pty Ltd.	• Press releases • Public website
Internal	Access to internal information is approved by management and is protected from external access.	• Internal memos • Design documents • Product specifications • Correspondences

Customer data	Information received from customers for processing or storage by Vyro Pty Ltd. Vyro Pty Ltd. must uphold the highest possible levels of integrity, confidentiality, and restricted availability for this information.	• Customer operating data • Customer PII • Customers' PII • Anything subject to a confidentiality agreement with a customer
Company data	Information collected and used by Vyro Pty Ltd. to operate the business. Vyro Pty Ltd. 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 which is utilized by the company in delivering its services.

All employees and contractors of the company are obligated to respect and, in all cases, protect customer data.

Additionally, Vyro Pty Ltd. has policies and procedures in place for the proper and secure handling of customer data. These policies and procedures are reviewed on at least an annual basis.

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

Physical Security

Vyro Pty Ltd.’s production servers are maintained by AWS. The physical and environmental security protections are the responsibility of AWS. Vyro Pty Ltd. reviews the attestation reports and performs a risk analysis of AWS on at least an annual basis.

Logical Access

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

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 the least privileged access.

The engineering Team is responsible for providing access to the system based on the employee's role and performing a background check. The employee is responsible for reviewing Vyro Pty Ltd.'s policies and completing security training. These steps must be completed within 1 day of hire.

When an employee is terminated, Engineering Team is responsible for de-provisioning access to all in-scope systems within 1 day of that employee's termination.

Computer Operations - Backups

Customer data is backed up and monitored by the Engineering Team for completion and exceptions. If there is an exception, Engineering Team 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 AWS with physical access restricted according to the policies. Backups are encrypted, with access restricted to key personnel.

Computer Operations - Availability

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

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

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

Change Management

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

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing and User Acceptance Testing (UAT) results are documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment. Management approves changes prior to migration to the production environment and documents those approvals within the ticketing system.

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

Data Communications

Vyro Pty Ltd. has elected to use a platform-as-a-service (PaaS) to run its production infrastructure in part to avoid the complexity of network monitoring, configuration, and operations. The PaaS simplifies our logical network configuration by providing an effective firewall around all the Vyro Pty Ltd. application containers, with the only ingress from the network via HTTPS connections to designated web frontend endpoints.

The PaaS provider also automates the provisioning and de-provisioning 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 the underlying hardware.

Vyro uses an automated monitoring service to perform weekly vulnerability scans and engages an external firm to perform annual penetration testing to look for unidentified vulnerabilities, and the product engineering team responds to any issues identified via the regular incident response and change management process.

BOUNDARIES OF THE SYSTEM

The boundaries of Vyro 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 Vyro.

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

THE APPLICABLE TRUST SERVICES CRITERIA AND THE RELATED CONTROLS

Common Criteria (to the Security Category)
Security refers to the protection of information during its collection or creation, use, processing, transmission, and storage and systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removals of information or system resources, misuse of the software, and improper access to or use of, alteration, destruction, or disclosure of information.

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 Vyro Pty Ltd.'s control environment, affecting the design, administration, and monitoring of other components. Integrity and ethical behavior are the product of Vyro Pty Ltd.'s ethical and behavioral standards, how they are communicated, and how they are reinforced in practice. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements and codes of conduct, as well as by example.

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

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

Commitment to Competence

Vyro Pty Ltd.'s management defines competence as the knowledge and skills necessary to accomplish tasks that define employees' roles and responsibilities. Management's commitment to competence includes

management's consideration of the competence levels for jobs and how those levels translate into the requisite skills and knowledge.

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

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

Management's Philosophy and Operating Style

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

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

Vyro Pty Ltd.'s assignment of authority and responsibility activities includes factors such as how authority and responsibility for operating activities are assigned and how reporting relationships and authorization hierarchies are established. It also includes policies relating to appropriate business practices, knowledge, and experience of key personnel, and resources provided for carrying out duties. In addition, it includes policies and communications directed at ensuring personnel understand the entity's objectives, know how their individual actions interrelate and contribute to those objectives, and recognize how and for what they will be held accountable.

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

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

HR Policies and Practices

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

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

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

RISK ASSESSMENT PROCESS

Vyro Pty Ltd.’s risk assessment process identifies and manages risks that could potentially affect Vyro Pty Ltd.’s ability to provide reliable and secure services to our customers. As part of this process, Vyro Pty Ltd. maintains a risk register to track all systems and procedures that could present risks to meeting the company’s objectives. Risks are evaluated by likelihood and impact, and management creates tasks to address risks that score highly on both dimensions. The risk register is reevaluated annually, and tasks are incorporated into the regular Vyro Pty Ltd. product development process so they can be dealt with predictably and iteratively.

Integration with Risk Assessment

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

INFORMATION AND COMMUNICATION SYSTEMS

Information and communication are an integral component of Vyro Pty Ltd.'s internal control system. It is the process of identifying, capturing, and exchanging information in the form and time frame necessary to conduct, manage, and control the entity's operations.

Vyro Pty Ltd. uses several information and communication channels internally to share information with management, employees, contractors, and customers. Vyro Pty Ltd. 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, Vyro Pty Ltd. uses in-person and video "all hands" meetings to communicate company priorities and goals from management to all employees.

MONITORING CONTROLS

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

On-going Monitoring

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

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

Reporting Deficiencies

Our internal risk management tracking tool is utilized to document and track the results of ongoing 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.

CHANGES TO THE SYSTEM

No significant changes have occurred to the services provided to user entities in the specified period.

INCIDENTS

No significant incidents have occurred to the services provided to user entities in the specified period.

CRITERIA NOT APPLICABLE TO THE SYSTEM

All Common Criteria/Security and Security criteria were applicable to Vyro Pty Ltd.'s Vyro system.

SUBSERVICE ORGANIZATIONS

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

SUBSERVICE DESCRIPTION OF SERVICES

The Cloud Hosting Services provided by AWS support the physical infrastructure of the entity's services.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

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

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

AWS

Category	Criteria	Control
Security	CC 6.4	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.
		Physical access to data centers is reviewed on a quarterly basis by the appropriate personnel.
		Closed-circuit television cameras (CCTV) are used to monitor server locations in data centers. Images are retained for 90 days unless limited by legal or contractual obligations.
		Access to server locations is managed by electronic access control devices.

Vyro Pty Ltd. 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, Vyro Pty Ltd. performs monitoring of the subservice organization controls, including the following procedures:

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

COMPLEMENTARY USER ENTITY CONTROLS

Vyro Pty Ltd.'s services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all the Trust Services Criteria related to Vyro Pty Ltd.'s services to be solely achieved by Vyro Pty Ltd. control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Vyro Pty Ltd.

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

IV. Description of Design of Controls and Results Thereof

Description of Design of Controls and Results Thereof

Relevant trust services criteria and Vyro Pty Ltd.-related controls are an integral part of management's system description and are included in this section. Johanson Group LLP performed testing to determine if Vyro Pty Ltd.'s controls were suitably designed to achieve the specified criteria for the security categories set forth in TSP Section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria),* as of September 28, 2022.

Tests of the criterion and controls included inquiry of appropriate management, supervisory and staff personnel, observation of Vyro Pty Ltd. activities and operations, and inspection of Vyro Pty Ltd. documents and records. The results of those tests were considered in the planning, the nature, timing, and extent of Johanson LLP's testing of the controls designed to achieve the relevant trust services criteria.

Criteria Number	Trust Criteria Services	Description of Vyro Pty Ltd.'s Controls	Test Result
CONTROL ENVIRONMENT			
CC 1.1	COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
		The company performs background checks on new employees.	Control determined to be suitably designed.
		The company requires contractor agreements to include a code of conduct or reference to the company code of conduct.	Control determined to be suitably designed.
		The company requires contractors to sign a confidentiality agreement at the time of engagement.	Control determined to be suitably designed.
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Control determined to be suitably designed.
		The company requires employees to sign a confidentiality agreement during onboarding.	Control determined to be suitably designed.
CC 1.2	COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	The company management demonstrates a commitment to integrity and ethical values.	Control determined to be suitably designed.

CC 1.3	COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company maintains an organizational chart that describes the organizational structure and reporting lines.	Control determined to be suitably designed.
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Control determined to be suitably designed.
CC 1.4	COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
		The company performs background checks on new employees.	Control determined to be suitably designed.
		The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Control determined to be suitably designed.
CC 1.5	COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company managers are required to complete performance evaluations for direct reports at least annually.	Control determined to be suitably designed.
		The company requires employees to acknowledge a code of conduct at the time of hire. Employees who violate the code of conduct are subject to disciplinary actions in accordance with a disciplinary policy.	Control determined to be suitably designed.
COMMUNICATION AND INFORMATION			
CC 2.1	COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Control determined to be suitably designed.

		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Control determined to be suitably designed.
CC 2.2	COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company communicates system changes to authorized internal users.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company management has established defined roles and responsibilities to oversee the design and implementation of information security controls.	Control determined to be suitably designed.
		The company provides a description of its products and services to internal and external users.	Control determined to be suitably designed.
		The company requires employees to complete security awareness training within thirty days of hire and annually thereafter.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
CC 2.3	COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	The company has an external-facing support system in place that allows users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel.	Control determined to be suitably designed.
		The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Control determined to be suitably designed.
		The company notifies customers of critical system changes that may affect their processing.	Control determined to be suitably designed.
		The company provides a description of its products and services to internal and external users.	Control determined to be suitably designed.
		The company provides guidelines and technical support resources relating to system operations to customers.	Control determined to be suitably designed.

		The company's security commitments are communicated to customers in Master Service Agreements (MSA) or Terms of Service (TOS).	Control determined to be suitably designed.
RISK ASSESSMENT			
CC 3.1	COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Control determined to be suitably designed.
CC 3.2	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.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
CC 3.3	COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
CC 3.4	COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Control determined to be suitably designed.

		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
MONITORING ACTIVITIES			
CC 4.1	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.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
CC 4.2	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.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		The company performs control self-assessments at least annually to gain assurance that controls are in place and operating effectively. Corrective actions are taken based on relevant findings.	Control determined to be suitably designed.
CONTROL ACTIVITIES			
CC 5.1	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.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.

		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
CC 5.2	COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
CC 5.3	COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in job descriptions and/or the Roles and Responsibilities policy.	Control determined to be suitably designed.
		The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.

		The company specifies its objectives to enable the identification and assessment of risk related to the objectives.	Control determined to be suitably designed.
		The company's data backup policy documents requirements for the backup and recovery of customer data.	Control determined to be suitably designed.
		The company's information security policies and procedures are documented and reviewed at least annually.	Control determined to be suitably designed.
LOGICAL AND PHYSICAL ACCESS			
CC 6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.
		The company has a data classification policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.	Control determined to be suitably designed.
		The company maintains a formal inventory of production system assets.	Control determined to be suitably designed.
		The company requires authentication to production datastores to use authorized secure authentication mechanisms, such as a unique SSH key.	Control determined to be suitably designed.
		The company requires authentication to systems and applications to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company requires passwords for in-scope system components to be configured according to the company's policy.	Control determined to be suitably designed.
		The company restricts access to migrate changes to production to authorized personnel.	Control determined to be suitably designed.
		The company restricts privileged access to databases to authorized users with a business need.	Control determined to be suitably designed.

		The company restricts privileged access to encryption keys to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the application to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the firewall to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the operating system to authorized users with a business need.	Control determined to be suitably designed.
		The company restricts privileged access to the production network to authorized users with a business need.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Control determined to be suitably designed.
		The company's datastores housing sensitive customer data are encrypted at rest.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Control determined to be suitably designed.
CC 6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
		The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.

		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Control determined to be suitably designed.
CC 6.3	The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
		The company conducts quarterly access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company ensures that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.	Control determined to be suitably designed.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company's access control policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.	Control determined to be suitably designed.
CC 6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	The entity does not operate any physical hardware such as servers and network devices but rather uses subservice organizations and relies on its own controls for physical access.	Control determined to be suitably designed.
CC 6.5	The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	The company completes termination checklists to ensure that access is revoked for terminated employees within SLAs.	Control determined to be suitably designed.
		The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.	Control determined to be suitably designed.
		The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.	Control determined to be suitably designed.

		The company purges or removes customer data containing confidential information from the application environment, in accordance with best practices, when customers leave the service.	Control determined to be suitably designed.
CC 6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		The company requires authentication to the "production network" to use unique usernames and passwords or authorized Secure Socket Shell (SSH) keys.	Control determined to be suitably designed.
		The company reviews its firewall rulesets at least annually. Required changes are tracked to completion.	Control determined to be suitably designed.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Control determined to be suitably designed.
		The company uses firewalls and configures them to prevent unauthorized access.	Control determined to be suitably designed.
		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Control determined to be suitably designed.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.	Control determined to be suitably designed.
		The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.	Control determined to be suitably designed.
CC 6.7	The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	The company encrypts portable and removable media devices when used.	Control determined to be suitably designed.
		The company has a mobile device management (MDM) system in place to centrally manage mobile devices supporting the service.	Control determined to be suitably designed.

		The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.	Control determined to be suitably designed.
CC 6.8	The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.	Control determined to be suitably designed.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
SYSTEM OPERATIONS			
CC 7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.	Control determined to be suitably designed.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.

CC 7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	An infrastructure monitoring tool is utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.	Control determined to be suitably designed.
		Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		The company uses an intrusion detection system to provide continuous monitoring of the company's network and early detection of potential security breaches.	Control determined to be suitably designed.
		The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.	Control determined to be suitably designed.
		The company's formal policies outline the requirements for the following functions related to IT / Engineering: - vulnerability management; - system monitoring.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
CC 7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
CC 7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.

		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company tests its incident response plan at least annually.	Control determined to be suitably designed.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
CC 7.5	The entity identifies, develops and implements activities to recover from identified security incidents.	The company has a documented business continuity/disaster recovery (BC/DR) plan and tests it at least annually.	Control determined to be suitably designed.
		The company has security and privacy incident response policies and procedures that are documented and communicated to authorized users.	Control determined to be suitably designed.
		The company tests its incident response plan at least annually.	Control determined to be suitably designed.
		The company's security and privacy incidents are logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.	Control determined to be suitably designed.
CHANGE MANAGEMENT			
CC 8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	Host-based vulnerability scans are performed at least quarterly on all external-facing systems. Critical and high vulnerabilities are tracked for remediation.	Control determined to be suitably designed.
		The company has a formal systems development life cycle (SDLC) methodology in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.	Control determined to be suitably designed.
		The company has infrastructure supporting the service patched as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.	Control determined to be suitably designed.
		The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.	Control determined to be suitably designed.

		The company restricts access to migrate changes to production to authorized personnel.	Control determined to be suitably designed.
		The company's network and system hardening standards are documented, based on industry best practices, and reviewed at least annually.	Control determined to be suitably designed.
		The company's penetration testing is performed at least annually. A remediation plan is developed and changes are implemented to remediate vulnerabilities in accordance with SLAs.	Control determined to be suitably designed.
RISK MITIGATION			
CC 9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	The company has a documented risk management program in place that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.	Control determined to be suitably designed.
		The company has Business Continuity and Disaster Recovery Plans in place that outline communication plans in order to maintain information security continuity in the event of the unavailability of key personnel.	Control determined to be suitably designed.
		The company's risk assessments are performed at least annually. As part of this process, threats and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.	Control determined to be suitably designed.
CC 9.2	The entity assesses and manages risks associated with vendors and business partners.	The company has a vendor management program in place. Components of this program include: - critical third-party vendor inventory; - vendor's security and privacy requirements; and - review of critical third-party vendors at least annually.	Control determined to be suitably designed.
		The company has written agreements in place with vendors and related third parties. These agreements include confidentiality and privacy commitments applicable to that entity.	Control determined to be suitably designed.