# Independent Assurance Report on Venn Services LLC's Description of its System and on the Suitability of the Design and Operating Effectiveness of its Controls Relevant to Security, Availability, and Confidentiality Trust Services Criteria (SOC 2)

**Prepared in accordance with the following:**

AT-C section 105: Concepts Common to All Attestation Engagements

AT-C section 205: Assertion-Based Examination Engagements

# Contents

# Section I

## ASSERTION OF VENN SERVICES LLC'S MANAGEMENT

## *ASSERTION OF VENN SERVICES LLC'S MANAGEMENT*

17 February 2025

We have prepared the accompanying description of Venn Services LLC's ('Venn Technology') Platform as a Service System (the 'Description') for the purposes of the independent assurance report. We have prepared the Description in accordance with the following description criteria ('Description Criteria'):

- SOC 2: 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) with regards to the Description.

The Description is intended to provide report users with information about the Venn Platform (the 'System') that may be useful when assessing the risks arising from interactions with Venn Technology's system. This includes the controls that Venn Technology has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (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).

Venn Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Venn Technology, to achieve Venn Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents Venn Technology's controls, the Agreed Criteria, and the types of complementary subservice organization controls assumed in the design of Venn Technology'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 are necessary, along with controls at Venn Technology, to achieve Venn Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents Venn Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Venn Technology's controls.

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

a. the Description presents Venn Platform was designed and implemented throughout the period 26 July 2024 to 26 January 2025 in accordance with the Description Criteria.
b. the controls stated in the Description were suitably designed throughout the period 26 July 2024 to 26 January 2025, to provide reasonable assurance that Venn Technology's service commitments and system requirements would be achieved based on the Agreed Criteria, if the controls operated effectively throughout that period, and if complementary subservice organization controls and complementary user entity controls assumed in the design of Venn Technology's controls operated effectively throughout that period; and
c. The controls stated in the Description operated effectively throughout the period 26 July 2024 to 26 January 2025, to provide reasonable assurance that Venn Technology's service commitments and system requirements were achieved based on the Agreed Criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of Venn Technology's controls operated effectively throughout that period.

Scott Hollrah

Scott Hollrah
Founder and CEO
Venn Services LLC

# Section II

## INDEPENDENT SERVICE AUDITOR'S REPORT

# *INDEPENDENT SERVICE AUDITOR'S REPORT*

To: Venn Services LLC's

**Scope**

We have examined Venn Services LLC's ('Venn Technology') accompanying description of its Platform as a Service System (the 'Description') which has been prepared for the purposes of the independent assurance report.

Venn Technology prepared the Description based on the following description criteria ('Description Criteria'):

- SOC 2: 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) with regards to the Description.

The Description is intended to provide report users with information about the Venn Platform (the 'System') that may be useful when assessing the risks arising from interactions with Venn Technology's system. This includes the controls that Venn Technology has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the following agreed criteria ('Agreed Criteria'):

- SOC 2: the trust services criteria relevant to Common Criteria/Security, Availability, and Confidentiality (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).

Venn Technology uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The Description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Venn Technology, to achieve Venn Technology's service commitments and system requirements based on the Agreed Criteria. The complementary subservice organization controls have been reviewed by Venn Technology management. 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 includes complementary user entity controls that are necessary, along with controls at Venn Technology, to achieve Venn Technology's service commitments and system requirements based on the Agreed Criteria. The Description presents Venn Technology's controls, the Agreed Criteria, and the complementary user entity controls assumed in the design of Venn Technology's controls. The complementary user entity controls have not been assessed by our examination and remain the responsibility of those related entities to complete their own review.

**Service Organization's Responsibilities**

Venn Technology 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 Venn Technology's service commitments and system requirements were achieved. Venn Technology has provided the accompanying assertion titled "Assertion of Venn Technology Management" (the 'Assertion') about the Description and the suitability of the design and operating effectiveness of the controls described therein to provide reasonable assurance that the service commitments and system requirements would be achieved based on the Agreed Criteria. Venn Technology 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 Agreed Criteria and

stating the related controls in the Description; and identifying the risks that threaten the achievement of the Venn Technology'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 AT-C 105 and AT-C 205 put forth by the Auditing Standards Board (ASB) of the American Institute of Certified Public Accountants (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.
- The controls stated in the Description were suitably designed.
- The controls stated in the Description were operating effectively throughout the period to provide reasonable assurance that Venn Technology's service commitments and system requirements were achieved based on the Agreed 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 Venn Technology's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and Venn Technology'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 Venn Technology achieved its service commitments and system requirements based on the Agreed Criteria.
- Testing the operating effectiveness of controls stated in the Description to provide reasonable assurance that Venn Technology achieved its service commitments and system requirements based on the Agreed Criteria.
- Evaluating the overall presentation of the Description.

**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.

Because of the inherent limitations of any internal control structure, it is possible that, even if the controls are suitably designed and implemented as designed, once the controls are in operation the control objectives may not be achieved so that fraud, error, or non-compliance with laws and regulations may occur and not be detected.

An assurance engagement on the implementation of controls at a specified date does not provide assurance on whether the controls operated effectively as designed or will operate effectively in the future. Any projection of the outcome of the evaluation of the suitability of the design and operating effectiveness of

controls to future periods is subject to the risk that the controls may become unsuitable because of changes in conditions.

**Opinion**

In our opinion, in all material respects,

1) the Description presents Venn Platform that was designed and implemented throughout the period 26 July 2024 to 26 January 2025, in accordance with the Description Criteria;
2) the controls stated in the Description were suitably designed throughout the period 26 July 2024 to 26 January 2025, to provide reasonable assurance that Venn Technology's service commitments and system requirements would be achieved based on the Agreed Criteria, if its controls operated effectively throughout that period and if the subservice organization and user entities applied the complementary controls assumed in the design of Venn Technology's controls throughout that period; and
3) The controls stated in the Description operated effectively throughout the period 26 July 2024 to 26 January 2025, to provide reasonable assurance that Venn Technology's service commitments and system requirements were achieved based on the Agreed Criteria, if the subservice organizations and user entities applied the complementary controls assumed in the design of Venn Technology's controls operated effectively throughout that period.

**Restricted Use**

This report is intended solely for the information and use of Venn Technology, user entities of Venn Platform, business partners of Venn Technology subject to risks arising from interactions with the Platform as a Service 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
- Complementary user entity controls and complementary subservice organization controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements
- User entity responsibilities and how they may affect the user entity's ability to effectively use the service organization's services
- The Agreed 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.

AssuranceLab CPAs LLC
Austin, Texas
United States
17 February 2025

# Section III

## VENN SERVICES LLC'S DESCRIPTION OF ITS SYSTEM

# OVERVIEW OF OPERATIONS

## Company Background

Venn Services LLC ('Venn Technology') was founded in January 2015 with the objective of providing expert Salesforce and integration services. Venn Technology is a global integration services firm with a global customer base, supporting clients across multiple software industry sectors.

## Description of Services Provided

Venn Technology supports customers across the United States, United Kingdom, Europe, Canada, New Zealand, and Australia.

Venn Technology's product, the Venn Platform, is a platform that allows for building, running, maintaining, and supporting real-time integrations that connect disparate software systems.

## Principal Service Commitments and System Requirements

Venn Technology has established processes, policies, and procedures to meet its objectives related to its Platform as a Service System (the 'System'). Those objectives are based on the purpose, vision, and values of Venn Technology as well as commitments that Venn Technology makes to user entities, the requirements of laws and regulations that apply to Venn Technology's activities, and the operational requirements that Venn Technology has established.

Commitments are documented, and communicated in customer agreements, as well as in public descriptions of the System. The operational requirements are communicated in Venn Technology's processes, policies and procedures, system design documentation, and customer agreements. This includes policies around how the System is designed and developed, how the System is operated, how the system components are managed, and how employees are hired, developed, and managed to support the System.

## Components of the System

### Infrastructure

Venn Technology's primary infrastructure used to provide the System includes the cloud hosted networking, compute and database components of AWS.

| System | Type | Description |
|---|---|---|
| **Amazon Elastic Compute Cloud (EC2)** | Cloud Compute | Secure and resizable compute capacity (virtual servers) in the cloud. |
| **Amazon Elastic Container Service (ECS)** | Cloud Compute | Secure, reliable, and scalable service to run containers. |
| **PostgreSQL** | Data storage | Open-source relational database management system emphasizing extensibility and SQL compliance. |
| **Amazon RDS** | Data storage | Relational database service. |
| **Amazon Simple Storage Service (S3)** | Data storage | Object, file, and block storage. |

| System | Type | Description |
|---|---|---|
| **AWS Web Application Firewall** | Web Application Firewall | Protects web applications or APIs against common web exploits and bots that may affect availability, compromise security, or consume excessive resources. |
| **AWS Elastic Load Balancing (ELB)** | Networking | Automatically distributes incoming application traffic across multiple targets. |
| **AWS Certificate Manager** | Encryption | A service to provision, manage, and deploy public and private Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificates for use with AWS services. |
| **AWS Key Management Service** | Key Management | Centralized control over the cryptographic keys used to protect data. |
| **Amazon Elastic Container Service (ECS)** | Cloud Compute | Secure, reliable, and scalable service to run containers. |

### Software

Primary software is used to support Venn Technology's system.

| Software | Purpose |
|---|---|
| **Venn Platform** | The software as a service product provided to Venn Technology customers. |
| **AWS CloudTrail** | Enables auditing, security monitoring, and operational troubleshooting by tracking user activity and API usage on AWS. |
| **AWS CloudWatch** | Monitoring and management service that provides data and actionable insights for AWS, hybrid, and on-premises applications and infrastructure resources. |
| **AWS GuardDuty** | Threat detection service that continuously monitors AWS accounts and workloads for malicious activity and delivers detailed security findings for visibility and remediation. |
| **AWS Security Token Service** | A web service to request temporary, limited-privilege credentials for AWS Identity and Access Management (IAM) users or for federated users. |
| **UniFi Enterprise Identity** | Authentication software used to identify and authenticate users for access control to the systems. |
| **GitHub** | Source code repository used to manage the software code and version control. |

| Software | Purpose |
|---|---|
| **GitHub Actions** | Continuous integration / continuous delivery software used to manage the pipeline of change release testing and deployment. |
| **1Password** | Enterprise password manager used to store authentication secrets and strengthen password security. |
| **Apple Business Manager** | Mobile device management software used to track and manage security policies on endpoint devices. |
| **XProtect** | Anti-virus software used to protect endpoint devices from malware. |
| **Rollbar** | System monitoring software used to log events and raise alerts to support system security and availability. |
| **GitHub Dependabot** | Vulnerability scanning software to identify, log and resolve technical vulnerabilities. |
| **Salesforce** | Ticketing software used to log events and requirements to support the internal controls. |
| **Gusto, Ethos Systems** | Human resources information system used to manage employee processes like onboarding, offboarding, and performance. |
| **Google Workspace** | Google's suite of enterprise productivity, collaboration, and communication tools. |
| **Drata** | Security and compliance software used to monitor and manage the security, risk, and control activities to support compliance. |

### People

Venn Technology has 30 people that are organized into the following functional areas:

- Leadership: The executive level responsible for corporate governance.
- Product: Responsible for managing the roadmap of products and Venn Platform enhancements while balancing the Engineering team priorities.
- Engineering: Responsible for building, supporting and maintaining the Venn Platform infrastructure and software.
- Customer Success: Responsible for the customer experience, support and services.
- Implementations: Responsible for enterprise implementations and integrations to onboard and set up new customers.
- Project Management: Responsible for enterprise delivery of products and projects to support the objectives.
- Operations: Responsible for monitoring and supporting robust and effective company and system operations.
- Partnerships: Responsible for managing partnerships with complimentary service providers.
- Sales: Responsible for onboarding new customers and aligning requirements.
- Marketing: Responsible for branding, market positioning, and attracting customers.

### Data

The data collected and processed by Venn Technology includes the following types:

- Basic personal details: name, email, contact details
- User activity: user activity within the software
- Financial account information: account balances, transactions
- Business information: proprietary data of business activities and property
- Sensitive personal information: personal characteristics, preferences, beliefs

## *Processes, Policies and Procedures*

Processes, policies, and procedures are established that set the standards and requirements of the System. All personnel are expected to comply with Venn Technology's policies and procedures that define how the System should be managed. The documented policies and procedures are shared with all Venn Technology's employees and can be referred to as needed.

### Compliance Management Platform

Venn Technology uses compliance automation software, Drata, to support the design, implementation, operation, monitoring, and documentation of internal controls. Drata leverages APIs to centralize the monitoring of Venn Technology's information assets across their infrastructure provider, identity manager, code repository, and endpoint devices. These APIs in combination with compliance automation functions in Drata supports the continuous monitoring of control activities for Venn Technology's people, devices, policies, procedures and plans, risk assessments, third-party vendor assessments, system monitoring and the security configurations of these critical systems.

Using Drata does not reduce management's responsibility for designing, implementing and operating an effective system of internal control. Venn Technology evaluates the accuracy and completeness of the information stored in Drata and conducts annual vendor risk assessments including review of Drata's SOC 2 Type 2 report that includes the trust services criteria related to processing integrity.

### Logical Access

Venn Technology's logical access processes restrict access to the infrastructure, software and data to only those that are authorized for access. Access is based on the concept of least privilege that limits the system components and access privileges to the minimum level required to fulfill job responsibilities.

The in-scope systems require approval and individual authentication practices prior to gaining access. UniFi Enterprise Identity authentication software is used for identity management and single-sign on. Access management processes are followed to ensure new and modified access is approved, terminated users access is removed, and access rights are reviewed quarterly and adjusted when no longer required. Additional information security policies and procedures require Venn Technology employees to use the systems and data in an appropriate and authorized manner.

Automated and manual security practices are used to protect the perimeter security and network to prevent unauthorized access attempts and tampering from third-party actors with malicious intent. Those include applying encryption of data and communications, periodic testing for and remediation of technical vulnerabilities and applying network controls like firewalls and event monitoring to prevent and detect unauthorized activity.

Venn Technology employee workstations are required to follow defined security practices to mitigate the risks of data leakage and malware that may compromise the devices, system access and sensitive data. Apple Business Manager mobile device management software is used to monitor, systematically enforce device requirements, and provide remote management capabilities for the workstations.

### System Operations

Backup and restoration procedures for the System are defined and followed. The System is monitored through a combination of automated and manual processes to prevent and detect any issues with the infrastructure, software, and data. Alerts and logs are monitored with incident management processes defined for handling and resolving adverse events.

Venn Technology's critical infrastructure and data are hosted by AWS with multiple availability zones to provide failover capability in the event of an outage of one of the data centers. Redundancy, disaster recovery in continuity considerations are built into the system design of AWS to support Venn Technology's availability objectives. These are supported by the system monitoring, incident management processes and defined recovery and continuity plans.

### Change Control

Venn Technology operates a defined process for software development with supporting policies and procedures. Change requests and requirements are logged and prioritized for development. Changes include those related to functionality improvements, bug fixes, security and reliability-related enhancements, and other updates to the Venn Platform software to support Venn Technology's System and objectives.

Separate environments are used to support development and testing activities in isolation from the production environment. GitHub version control software is used for the code repository that tracks all changes to the Venn Platform software, including managing versions and roll-back capability in the event of a failed change release. Branch production rules and a continuous integration / continuous deployment (CI/CD) pipeline is configured using GitHub Actions to enforce key process steps and checks prior to new versions of the code base being deployed into the production environment. Changes to the infrastructure configurations and settings are managed as code, subject to the same process steps and checks prior to impacting the production environment.

### Data Governance

Venn Technology uses data to support the System objectives and services. An approach to effective data governance has been established to understand and communicate the data that's used in the System, the objectives and requirements of that data, and the commitments of Venn Technology.

Established processes, policies, procedures define the operational requirements for data governance, including how data is classified, handled, and used by the System in supporting the objectives and services.

## *Boundaries of the System*

The scope of this report includes the Venn Platform (the 'System'). This report does not include the cloud hosting services provided by AWS.

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

### Integrity and Ethical Values

The effectiveness of controls is dependent on the integrity and ethical values of the people who implement, manage, and monitor them. Integrity and ethical values are important foundations of Venn Technology's control environment, affecting the design, implementation, and monitoring of the controls. Integrity and ethical behavior are supported by Venn Technology's culture, governance, hiring and onboarding practices, ethical and behavioral standards, the way those 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.

### Commitment to Competence

Venn Technology's competence of employees includes the knowledge and skills necessary to accomplish employees' roles and responsibilities, in support of Venn Technology's objectives and commitments. Management's commitment to competence includes careful consideration of the competence levels required for each role, the requisite skills, knowledge, and experience, and the actual performance of individuals, teams and the company as a whole.

### Management's Philosophy and Operating Style

Venn Technology's management philosophy and operating style is a purpose-driven, risk-based approach to pursuing the company objectives and satisfying Venn Technology's commitments. Risk taking is an essential part of pursuing the objectives. A formal approach is taken to understanding those risks and being deliberate about which risks are acceptable, and where risk mitigation actions are required.

### Organizational Structure and Assignment of Authority and Responsibility

Venn Technology's organizational structure provides the framework within which its activities for achieving the objectives are planned, executed, managed, and monitored. An organizational structure has been developed to suit Venn Technology's needs and is revised over time as the company grows and requirements change.

Roles and responsibilities are further established and communicated through documented policies and job descriptions, as part of individual performance review processes, reviewing and communicating team and functional performance, and the various operational team and governance meetings.

### Human Resource Policies and Practices

Venn Technology's employees are the foundation for achieving the objectives and commitments. Venn Technology's hiring, onboarding, and human resource practices are designed to attract, develop, and retain high-quality employees. That includes training and development, performance evaluations, compensation and promotions, providing personal support and perks for individuals, recognizing team and company success, and building a culture of alignment to a shared purpose and vision. It also includes disciplinary processes and business planning to avoid single-person dependencies to ensure the objectives and commitments are not reliant on individuals.

## *Risk Assessment Process*

### Risk Assessments

Venn Technology's risk assessment process identifies and manages risks that threaten achievement of the objectives and commitments. This includes risks that may affect the security, reliability or integrity of the services provided to user organizations and other interested stakeholders.

A formal process is followed to identify, assess, treat, and monitor the risks to ensure the risks are aligned to the risk appetite and objectives of Venn Technology, and mitigated or avoided where appropriate. Risks identified in this process include:

- Operational risk – changes in the environment, staff, or management personnel, reliance on third parties, and threats to security, reliability, and integrity of Venn Technology's operations.
- Strategic risk – new technologies, changing business models, and shifts within the industry.
- Compliance – legal and regulatory obligations and changes.
- Financial – the sustainability of Venn Technology and resources supporting the objectives.

These risks are identified by Venn Technology management, employees, and third-party stakeholders, and updated in the risk register as a single source of monitoring the risks. The formal risk assessments ensure the ongoing commitment of management, and support completeness and an evolving view of the risk landscape in Venn Technology's context.

**Integration with Risk Assessment**

Established internal controls include Venn Technology's policies, procedures, automated system functions and manual activities. The controls are designed and implemented to address the identified risks, and to meet the obligations and criteria set by laws, regulations, customer commitments and other compliance obligations. The controls follow a continual improvement methodology in consideration of the costs and benefits of such control improvements and recognizing the changing landscape and requirement of those controls as Venn Technology grows and the associated risks change.

## *Information and Communications Systems*

Information and communication are a core part of Venn Technology'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 Venn Technology's operations effectively. The information and communication systems consider the internal control requirements, operating requirements, and the needs of interested parties including employees, customers, third-party vendors, regulators, and stakeholders.

The information and communication systems include central tracking systems that support Venn Technology's established processes, as well as various meetings, and documented policies, procedures and organizational knowledge.

## *Monitoring Controls*

Management monitors the controls to ensure that they are operating as intended and that controls are modified and continually improved over time. Leadership, culture, and communication of the controls are important enablers to the effectiveness of the controls in practice. This ensures buy-in amongst the employees and empowers Venn Technology's team and individuals to prioritize the performance and continual improvement of the controls. Evaluations are performed during the course of business, in management reviews, and by independent auditors to assess the design and operating effectiveness of the controls. Deficiencies that are identified are communicated to responsible control owners to agree remediation actions or re-enforce the control requirements and importance. Corrective actions are tracked with agreed timelines and ownership for remediation with ownership of management and owners, for ensuring appropriate actions are completed in a timely manner.

## *Changes to the System in the Last 12 Months*

No significant changes have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

### *Incidents in the Last 12 Months*

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review date.

### *Criteria Not Applicable to the System*

All Common Criteria/Security, Availability, Confidentiality Trust Services Criteria were applicable to Venn Technology's Platform.

# COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS

This report does not include the cloud hosting services provided by AWS.

## Subservice Description of Services

AWS provides a highly reliable, scalable, low-cost infrastructure platform in the cloud that powers hundreds of thousands of businesses in 190 countries around the world. With data center locations in the U.S., Europe, Brazil, Singapore, Japan, and Australia.

## Complementary Subservice Organization Controls

Venn Technology'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 Agreed Criteria related to Venn Technology's services to be solely achieved by Venn Technology control procedures. Accordingly, subservice organizations, in conjunction with the services, should establish their own internal controls or procedures to complement those of Venn Technology.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the Agreed Criteria described within this report are met.

| Subservice Organization – AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| Common Criteria/ Security | CC6.1-CC6.8 | Logical access measures are established and followed to ensure access to systems and data is restricted to authorized personnel with technical safeguards and ongoing assessments to reduce the risk of system and data breaches. |
| Common Criteria/ Security | CC6.4 | 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 appropriate personnel. |
| | | Physical access points to server locations are recorded by closed circuit television camera ('CCTV'). Images are retained for 90 days, unless limited by legal or contractual obligations. |
| | | Physical access points to server locations are managed by electronic access control devices. |
| | | Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. |
| Common Criteria/ Security | CC7.1-CC7.5 | Incident management and response policies and procedures are established and followed to identify, analyze, classify, respond to and resolve adverse events. |
| Common Criteria/ Security | CC8.1 | Formal processes are established and followed to ensure system changes are documented, tracked, prioritized, developed, tested and approved prior to deployment into production. |
| Availability | A1.2 | Amazon-owned data centers are protected by fire detection and suppression systems. |

| Subservice Organization – AWS | | |
|---|---|---|
| **Category** | **Criteria** | **Control** |
| | | Amazon-owned data centers are air conditioned to maintain appropriate atmospheric conditions. Personnel and systems monitor and control air temperature and humidity at appropriate levels. |
| | | Uninterruptible Power Supply ('UPS') units provide backup power in the event of an electrical failure in Amazon-owned data centers. |
| | | Amazon-owned data centers have generators to provide backup power in case of electrical failure. |
| | | Contracts are in place with third-party colocation service providers which include provisions to provide fire suppression systems, air conditioning to maintain appropriate atmospheric conditions, Uninterruptible Power Supply (UPS) units, and redundant power supplies. |
| | | AWS performs periodic reviews of colocation service providers to validate adherence with AWS security and operational standards. |
| | | If enabled by the customer, RDS backs up customer databases, stores backups for user-defined retention periods, and supports point-in-time recovery. |
| | | Critical AWS system components are replicated across multiple Availability Zones and backups are maintained. |

Venn Technology management, along with the subservice organization, define the scope and responsibility of the controls necessary to meet all the relevant Agreed Criteria through written contracts and published terms of service. In addition, Venn Technology performs monitoring of the subservice organization controls by reviewing attestation reports and monitoring the performance of the subservice organization controls.

## *COMPLEMENTARY USER ENTITY CONTROLS*

Venn Technology'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 of the Agreed Criteria related to Venn Technology's services to be solely achieved by Venn Technology control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of Venn Technology's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Agreed 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.

User entities are responsible for:

- Understanding and complying with Venn Technology's terms of service.
- Notifying Venn Technology of changes made to technical or administrative contact information.
- Administering their users' access rights including approval, removal, and periodic review to ensure access is appropriate.
- Configuring minimum password settings and ensuring those settings meet their minimum requirements.
- Performing any required risk assessments and approvals when using pre-built integrations available with Venn Technology's services.
- Ensuring the supervision, management, and control of the use of Venn Technology's services by their personnel.
- Developing their own disaster recovery and business continuity plans that address the inability to access or utilize Venn Technology services for any critical reliance on these services.
- Immediately notifying Venn Technology of any actual or suspected information security breaches or system failures.

## *SOC 2 TRUST SERVICES CRITERIA*

### *Trust Services Categories Selected by Venn Technology*

| **Common Criteria (*to all Categories*)** |
|---|
| Security refers to the protection of<br>i. information during its collection or creation, use, processing, transmission, and storage and<br>ii. 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 removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information. |

| **Availability** |
|---|
| Availability refers to the accessibility of information used by the entity's systems, as well as the products or services provided to its customers. The availability objective does not, in itself, set a minimum acceptable performance level; it does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems). However, it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance. |

| **Confidentiality** |
|---|
| Confidentiality addresses the entity's ability to protect information designated as confidential from its collection or creation through its final disposition and removal from the entity's control in accordance with management's objectives. Information is confidential if the custodian (for example, an entity that holds or stores information) of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties (including those who may otherwise have authorized access within its system boundaries). Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons. For example, the information may be proprietary, intended only for entity personnel.<br><br>Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property. |

# Section IV

## CRITERIA AND RELATED CONTROLS

## SOC 2 TRUST SERVICES CRITERIA

### Trust Services Criteria for the Security Category

#### Common Criteria 1: Control Environment

| CC1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC1.1 | COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values. | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |
| | | Background checks are conducted for new hires. | Inspected the background checks for a sample of new hires to determine that background checks were conducted for new hires. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| | | Venn Technology establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment. | Inspected the code of conduct to determine that Venn Technology established workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment. | No exceptions noted. |

| CC1.0 | Criteria | Control Activity | 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. | Venn Technology's board of directors has a documented charter that outlines the roles, responsibilities, and key activities of the board. | Inspected the board charter to determine that Brevity's board of directors had a documented charter that outlined the roles, responsibilities, and key activities of the board. | No exceptions noted. |
| | | Venn Technology's board of directors meets at least annually and maintains meeting minutes. | Inspected the board meeting minutes to determine that Venn Technology's board of directors met at least annually and maintained meeting minutes. | No exceptions noted. |
| | | The documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | No exceptions noted. |
| CC1.3 | COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives. | Job descriptions are documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual. | Inspected the job descriptions for a sample of employees to determine that job descriptions were documented to support the hiring of suitable candidates and to communicate the key job responsibilities of each individual. | No exceptions noted. |
| | | The documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | No exceptions noted. |

| CC1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | Inspected the information security policies to determine that Venn Technology's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | No exceptions noted. |
| | | Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization. | Inspected the defined roles and responsibilities to determine that management had established defined roles and responsibilities to oversee implementation of the information security policy across the organization. | No exceptions noted. |
| CC1.4 | COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives. | Security awareness training is conducted for Venn Technology employees at least annually. | Inspected the records of security awareness training to determine that security awareness training was conducted for Venn Technology employees at least annually. | No exceptions noted. |
| | | Background checks are conducted for new hires. | Inspected the background checks for a sample of new hires to determine that background checks were conducted for new hires. | No exceptions noted. |
| | | Venn Technology evaluates the performance of all employees through a formal, annual performance review. | Inspected the performance reviews for a sample of employees to determine that Venn Technology evaluated the performance of all employees through a formal, annual performance review. | No exceptions noted. |
| | | Venn Technology establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a | Inspected the code of conduct to determine that Venn Technology established workforce conduct standards of integrity, ethical values, and appropriate behavior to support a secure and effective working environment. | No exceptions noted. |

| CC1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | secure and effective working environment. | | |
| CC1.5 | COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives. | Venn Technology evaluates the performance of all employees through a formal, annual performance review. | Inspected the performance reviews for a sample of employees to determine that Venn Technology evaluated the performance of all employees through a formal, annual performance review. | No exceptions noted. |
| | | The documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | No exceptions noted. |
| | | Management has established defined roles and responsibilities to oversee implementation of the information security policy across the organization. | Inspected the defined roles and responsibilities to determine that management had established defined roles and responsibilities to oversee implementation of the information security policy across the organization. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| | | Venn Technology establishes workforce conduct standards of integrity, ethical values, and appropriate behavior to support a | Inspected the code of conduct to determine that Venn Technology established workforce conduct standards of integrity, ethical values, and | No exceptions noted. |

| CC1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | secure and effective working environment. | appropriate behavior to support a secure and effective working environment. | |

## Common Criteria 2: Information and Communication

| CC2.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC2.1 | COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control. | Venn Technology maintains an architecture diagram to document the system boundaries and support the functioning of internal control. | Inspected the architecture diagram to determine that Venn Technology maintained an architecture diagram to document the system boundaries and support the functioning of internal control. | No exceptions noted. |
| | | Information logs related to the information processing activities are centrally stored for retrospective analysis where required. | Inspected the configuration of log capture to determine that information logs related to the information processing activities were centrally stored for retrospective analysis where required. | No exceptions noted. |
| | | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | Inspected the information asset register to determine that the information assets were identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | No exceptions noted. |
| | | Venn Technology has an established policy and procedures that governs the use of cryptographic controls. | Inspected the encryption policy to determine that Venn Technology had an established policy and procedures that governed the use of cryptographic controls. | No exceptions noted. |
| | | Venn Technology establishes the requirements for backups and recoverability. | Inspected the backup policy to determine that Venn Technology established the requirements for backups and recoverability. | No exceptions noted. |

| CC2.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |
| | | Security awareness training is conducted for Venn Technology employees at least annually. | Inspected the records of security awareness training to determine that security awareness training was conducted for Venn Technology employees at least annually. | No exceptions noted. |
| | | Venn Technology's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | Inspected the information security policies to determine that Venn Technology's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | No exceptions noted. |
| | | Venn Technology defines the contacts and methods for employees to report security-related incidents and concerns. | Inspected the responsible disclosure policy to determine that Venn Technology defined the contacts and methods for employees to report security-related incidents and concerns. | No exceptions noted. |

| CC2.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology defines the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | Inspected the incident response plans to determine that Venn Technology defined the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| CC2.3 | COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control. | Venn Technology follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | Inspected the incident handling for a sample of incidents to determine that Venn Technology followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | No exceptions noted. |
| | | Terms of service are agreed with Venn Technology's customers and users of the services to communicate their responsibilities and terms of use. | Inspected the terms of service to determine that terms of service were agreed with Venn Technology's customers and users of the services to communicate their responsibilities and terms of use. | No exceptions noted. |

| CC2.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | No exceptions noted. |
| | | Venn Technology defines the approach to identifying, assessing and resolving security vulnerabilities. | Inspected the vulnerability management policy to determine that Venn Technology defined the approach to identifying, assessing and resolving security vulnerabilities. | No exceptions noted. |
| | | Venn Technology defines the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | Inspected the incident response plans to determine that Venn Technology defined the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Venn Technology establishes the scope of information assets and requirements for how those are tracked and managed accordingly. | Inspected the asset management policy to determine that Venn Technology established the scope of information assets and requirements for how those were tracked and managed accordingly. | No exceptions noted. |

## Common Criteria 3: Risk Assessment

| CC3.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC3.1 | COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives. | The information security policies are reviewed by management at least annually and updated where required. | Inspected the review of the information security policies to determine that the information security policies were reviewed by management at least annually and updated where required. | No exceptions noted. |
| | | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |
| | | Venn Technology's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | Inspected the information security policies to determine that Venn Technology's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | No exceptions noted. |
| | | Venn Technology has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | Inspected the risk assessment policy to determine that Venn Technology had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | No exceptions noted. |
| CC3.2 | COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a | Venn Technology conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | Inspected the risk assessments to determine that Venn Technology conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | No exceptions noted. |

| CC3.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | basis for determining how the risks should be managed. | Venn Technology's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities. | Inspected the risk remediation plan to determine that Venn Technology's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities. | No exceptions noted. |
| | | The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | No exceptions noted. |
| | | Venn Technology performs security and compliance assessments of high-risk vendors. | Inspected the security and compliance review for a sample of high-risk vendors to determine that Venn Technology performed security and compliance assessments of high-risk vendors. | No exceptions noted. |
| | | Venn Technology has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | Inspected the risk assessment policy to determine that Venn Technology had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | No exceptions noted. |
| | | Venn Technology establishes the scope of information assets and requirements for how those are tracked and managed accordingly. | Inspected the asset management policy to determine that Venn Technology established the scope of information assets and requirements for how those were tracked and managed accordingly. | No exceptions noted. |

| CC3.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC3.3 | COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives. | Venn Technology conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | Inspected the risk assessments to determine that Venn Technology conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | No exceptions noted. |
| | | Venn Technology's management prepares a remediation plan to formally manage the resolution of findings identified in the risk assessment activities. | Inspected the risk remediation plan to determine that Venn Technology's management prepared a remediation plan to formally manage the resolution of findings identified in the risk assessment activities. | No exceptions noted. |
| | | Venn Technology has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | Inspected the risk assessment policy to determine that Venn Technology had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | No exceptions noted. |
| CC3.4 | COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control. | The documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | Inspected the organization chart to determine that the documented organization chart outlines the roles, functional responsibilities and reporting lines for Venn Technology personnel and demonstrates independence between management and the board of directors. | No exceptions noted. |
| | | Venn Technology conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | Inspected the risk assessments to determine that Venn Technology conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | No exceptions noted. |

| CC3.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology has defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | Inspected the risk assessment policy to determine that Venn Technology had defined a formal risk management process for evaluating risks based on identified threats, assessment criteria, existing internal controls and the risk tolerance. | No exceptions noted. |
| | | Venn Technology establishes the scope of information assets and requirements for how those are tracked and managed accordingly. | Inspected the asset management policy to determine that Venn Technology established the scope of information assets and requirements for how those were tracked and managed accordingly. | No exceptions noted. |

## Common Criteria 4: Monitoring Activities

| CC4.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | Inspected the Drata monitoring to determine that Drata was used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | No exceptions noted. |
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | Independent penetration tests are conducted annually. | Inspected the penetration test report to determine that independent penetration tests were conducted annually. | No exceptions noted. |
| CC4.2 | COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |

| CC4.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | parties responsible for taking corrective action, including senior management and the board of directors, as appropriate. | Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | Inspected the Drata monitoring to determine that Drata was used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | No exceptions noted. |
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | Independent penetration tests are conducted annually. | Inspected the penetration test report to determine that independent penetration tests were conducted annually. | No exceptions noted. |
| | | Venn Technology defines the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | Inspected the incident response plans to determine that Venn Technology defined the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | No exceptions noted. |

## Common Criteria 5: Control Activities

| CC5.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | Inspected the Drata monitoring to determine that Drata was used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | No exceptions noted. |
| | | Venn Technology conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | Inspected the risk assessments to determine that Venn Technology conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation 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. | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |

| CC5.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology conducts annual business continuity and disaster recovery tests to ensure the response plans are effective. | Inspected the business continuity and disaster recovery tests to determine that Venn Technology conducted annual business continuity and disaster recovery tests to ensure the response plans were effective. | No exceptions noted. |
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | Independent penetration tests are conducted annually. | Inspected the penetration test report to determine that independent penetration tests were conducted annually. | No exceptions noted. |
| | | Venn Technology conducts risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | Inspected the risk assessments to determine that Venn Technology conducted risk assessments at least annually to identify new and emerging risks, revise the existing risks, and devise risk mitigation actions. | No exceptions noted. |
| | | Venn Technology defines the contacts and methods for employees to report security-related incidents and concerns. | Inspected the responsible disclosure policy to determine that Venn Technology defined the contacts and methods for employees to report security-related incidents and concerns. | No exceptions noted. |

| CC5.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology requires role-based access control in line with the principle of least privilege where access rights are limited to the requirements of each role. | Inspected the access control policy to determine that Venn Technology required role-based access control in line with the principal of least privilege where access rights were limited to the requirements of each role. | No exceptions noted. |
| | | Venn Technology has an established policy and procedures that governs the use of cryptographic controls. | Inspected the encryption policy to determine that Venn Technology had an established policy and procedures that governed the use of cryptographic controls. | No exceptions noted. |
| 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. | The information security policies are reviewed by management at least annually and updated where required. | Inspected the review of the information security policies to determine that the information security policies were reviewed by management at least annually and updated where required. | No exceptions noted. |
| | | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |
| | | Venn Technology's set of information security policies cover the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | Inspected the information security policies to determine that Venn Technology's set of information security policies covered the roles, responsibilities, and requirements to support effective internal control that support the information security objectives. | No exceptions noted. |

## Common Criteria 6: Logical and Physical Access Controls

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology stores sensitive data, including customer data, in databases that are encrypted at rest. | Inspected the database encryption to determine that Venn Technology stored sensitive data, including customer data, in databases that were encrypted at rest. | No exceptions noted. |
| | | Multi-factor authentication is required for access to sensitive systems. | Inspected the monitoring of multi-factor authentication to determine that multi-factor authentication was required for access to sensitive systems. | No exceptions noted. |
| | | User accounts are individually assigned with a unique user ID to support system logging and accountability. | Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability. | No exceptions noted. |
| | | The information security policies are reviewed by management at least annually and updated where required. | Inspected the review of the information security policies to determine that the information security policies were reviewed by management at least annually and updated where required. | No exceptions noted. |
| | | The information security policies are communicated, read and acknowledged by employees. | Inspected the information security policies and monitoring of acknowledgements by employees to determine that the information security policies were communicated, read and acknowledged by employees. | No exceptions noted. |
| | | Venn Technology employees utilize a password manager to support quality passwords and secure authentication practices. | Inspected the monitoring of password managers installed on workstations to determine that Venn Technology employees utilized a password manager to support quality passwords and secure authentication practices. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology's workstations have hard-disk encryption applied to protect locally stored data and access credentials. | Inspected the monitoring of hard-disk encryption for devices to determine that Venn Technology's workstations have hard-disk encryption applied to protect locally stored data and access credentials. | No exceptions noted. |
| | | The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | Inspected the information asset register to determine that the information assets were identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | No exceptions noted. |
| | | Venn Technology requires role-based access control in line with the principle of least privilege where access rights are limited to the requirements of each role. | Inspected the access control policy to determine that Venn Technology required role-based access control in line with the principal of least privilege where access rights were limited to the requirements of each role. | No exceptions noted. |
| | | Venn Technology establishes the requirements for authentication including strong passwords, multi-factor and single sign-on as applicable to Venn Technology's systems. | Inspected the password policy to determine that Venn Technology established the requirements for authentication including strong passwords, multi-factor and single sign-on as applicable to Venn Technology's systems. | No exceptions noted. |
| | | Venn Technology has established formal guidelines for passwords to govern the management and use of authentication mechanisms. | Inspected the password policy to determine that Venn Technology has established formal guidelines for passwords to govern the management and use of authentication mechanisms. | No exceptions noted. |
| | | Venn Technology establishes the requirements for backups and recoverability. | Inspected the backup policy to determine that Venn Technology established the requirements for backups and recoverability. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | User accounts are individually assigned with a unique user ID to support system logging and accountability. | Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability. | No exceptions noted. |
| | | New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted. | Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted. | No exceptions noted. |
| | | A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner. | Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner. | No exceptions noted. |
| | | Venn Technology requires appropriate access approvals, periodic user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorized personnel. | Inspected the access control policy to determine that Venn Technology required appropriate access approvals, periodic user access reviews, and revocation of access in a timely manner upon termination, to ensure access was restricted to authorized personnel. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology requires role-based access control in line with the principle of least privilege where access rights are limited to the requirements of each role. | Inspected the access control policy to determine that Venn Technology required role-based access control in line with the principal of least privilege where access rights were limited to the requirements of each role. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| CC6.3 | The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, considering the concepts of least privilege and segregation of duties, to meet the entity's objectives. | User accounts are individually assigned with a unique user ID to support system logging and accountability. | Inspected the monitoring of unique user ID's to determine that user accounts were individually assigned with a unique user ID to support system logging and accountability. | No exceptions noted. |
| | | New hires and other new system access requirements are approved as part of the onboarding process or by authorized system owners prior to access being granted. | Inspected the access approval for a sample of new hires to determine that new hires and other new system access requirements were approved as part of the onboarding process or by authorized system owners prior to access being granted. | No exceptions noted. |
| | | A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner. | Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Quarterly reviews of Venn Technology's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required. | Inspected the user access review for a sample of quarters to determine that quarterly reviews of Venn Technology's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required. | No exceptions noted. |
| | | Venn Technology requires appropriate access approvals, periodic user access reviews, and revocation of access in a timely manner upon termination, to ensure access is restricted to authorized personnel. | Inspected the access control policy to determine that Venn Technology required appropriate access approvals, periodic user access reviews, and revocation of access in a timely manner upon termination, to ensure access was restricted to authorized personnel. | No exceptions noted. |
| | | Venn Technology requires role-based access control in line with the principle of least privilege where access rights are limited to the requirements of each role. | Inspected the access control policy to determine that Venn Technology required role-based access control in line with the principal of least privilege where access rights were limited to the requirements of each role. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | This criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC6.5 | The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives. | The information assets are identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | Inspected the information asset register to determine that the information assets were identified, classified, and centrally logged in Drata for ongoing monitoring and governance. | No exceptions noted. |
| | | A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner. | Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner. | No exceptions noted. |
| | | Quarterly reviews of Venn Technology's critical systems and associated user access rights are performed to ensure access is appropriate, or to modify access where required. | Inspected the user access review for a sample of quarters to determine that quarterly reviews of Venn Technology's critical systems and associated user access rights were performed to ensure access was appropriate, or to modify access where required. | No exceptions noted. |
| | | The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed. | Inspected the secure disposal policies and procedures to determine that the disposal of sensitive information assets followed a defined process to ensure sensitive data was effectively erased before the safeguards over the information assets were removed. | No exceptions noted. |
| | | Venn Technology establishes the requirements for backups and recoverability. | Inspected the backup policy to determine that Venn Technology established the requirements for backups and recoverability. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC6.6 | The entity implements logical access security measures to protect against threats from sources outside its system boundaries. | Access to cloud data storage is configured to restrict public access. | Inspected the cloud data storage configuration to determine that access to cloud data storage was configured to restrict public access. | No exceptions noted. |
| | | Venn Technology uses firewall configurations that ensure only approved networking ports and protocols can be used. | Inspected the firewall configurations to determine that Venn Technology used firewall configurations that ensured only approved networking ports and protocols could be used. | No exceptions noted. |
| | | A web application firewall configuration is used to protect Venn Technology's application from unauthorized access and external threats. | Inspected the web application firewall to determine that a web application firewall configuration was used to protect Venn Technology's application from unauthorized access and external threats. | No exceptions noted. |
| | | Connections and data flows to the Platform as a Service System and the supporting infrastructure are encrypted in transit. | Inspected the encryption in transit configurations to determine that connections and data flows to the Platform as a Service System and the supporting infrastructure were encrypted in transit. | No exceptions noted. |
| | | Venn Technology workstations apply screen lock with a timeout of no more than 15 minutes to prevent unauthorized viewing or access. | Inspected the monitoring of the configured screen lock to determine that Venn Technology workstations applied screen lock with a timeout of no more than 15 minutes to prevent unauthorized viewing or access. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology establishes the requirements for authentication including strong passwords, multi-factor and single sign-on as applicable to Venn Technology's systems. | Inspected the password policy to determine that Venn Technology established the requirements for authentication including strong passwords, multi-factor and single sign-on as applicable to Venn Technology's systems. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | Venn Technology stores sensitive data, including customer data, in databases that are encrypted at rest. | Inspected the database encryption to determine that Venn Technology stored sensitive data, including customer data, in databases that were encrypted at rest. | No exceptions noted. |
| | | Connections and data flows to the Platform as a Service System and the supporting infrastructure are encrypted in transit. | Inspected the encryption in transit configurations to determine that connections and data flows to the Platform as a Service System and the supporting infrastructure were encrypted in transit. | No exceptions noted. |
| | | Venn Technology's workstations have hard-disk encryption applied to protect locally stored data and access credentials. | Inspected the monitoring of hard-disk encryption for devices to determine that Venn Technology's workstations have hard-disk encryption applied to protect locally stored data and access credentials. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |

| CC6.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | No exceptions noted. |
| | | Antivirus software is installed on workstations to protect against malware. | Inspected the monitoring of antivirus software installed on workstations to determine that antivirus software was installed on workstations to protect against malware. | No exceptions noted. |
| | | Venn Technology's workstations operating system security patches are applied automatically. | Inspected the monitoring of automated operating system security patching to determine that Venn Technology's workstations operating system security patches were applied automatically. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |

## Common Criteria 7: System Operations

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology uses a version control system to manage source code, documentation, release labelling, and other change management tasks. | Inspected the version control software to determine that Venn Technology used a version control system to manage source code, documentation, release labelling, and other change management tasks. | No exceptions noted. |
| | | When Venn Technology's application code changes, code reviews and tests are performed by someone other than the person who made the code change. | Inspected the systematic enforcement of peer reviews to determine that when Venn Technology's application code changes, code reviews and tests were performed by someone other than the person who made the code change. | No exceptions noted. |
| | | Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | No exceptions noted. |
| | | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Independent penetration tests are conducted annually. | Inspected the penetration test report to determine that independent penetration tests were conducted annually. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | Information logs related to the information processing activities are centrally stored for retrospective analysis where required. | Inspected the configuration of log capture to determine that information logs related to the information processing activities were centrally stored for retrospective analysis where required. | No exceptions noted. |
| | | Infrastructure logging is configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | Inspected the infrastructure logging to determine that infrastructure logging was configured to monitor web traffic and suspicious activity with automated alerts raised for anomalous activity. | No exceptions noted. |
| | | Venn Technology conducts continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | Inspected the continuous monitoring in Drata to determine that Venn Technology conducted continuous monitoring of the security controls using Drata with automated alerts and tracking of the control effectiveness over time. | No exceptions noted. |
| | | Drata is used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | Inspected the Drata monitoring to determine that Drata was used to continuously monitor the security and compliance of its information assets including its people, systems, and control framework. | No exceptions noted. |

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | Independent penetration tests are conducted annually. | Inspected the penetration test report to determine that independent penetration tests were conducted annually. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | Venn Technology follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | Inspected the incident handling for a sample of incidents to determine that Venn Technology followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | No exceptions noted. |
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | Venn Technology has appointed an emergency response team to mobilize and manage incidents through to resolution. | Inspected the incident response plans to determine that Venn Technology had appointed an emergency response team to mobilize and manage incidents through to resolution. | No exceptions noted. |

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology defines the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | Inspected the incident response plans to determine that Venn Technology defined the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| 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. | Venn Technology follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | Inspected the incident handling for a sample of incidents to determine that Venn Technology followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | No exceptions noted. |
| | | Venn Technology has appointed an emergency response team to mobilize and manage incidents through to resolution. | Inspected the incident response plans to determine that Venn Technology had appointed an emergency response team to mobilize and manage incidents through to resolution. | No exceptions noted. |

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology defines the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | Inspected the incident response plans to determine that Venn Technology defined the roles, responsibilities and requirements for identifying, classifying, and resolving incidents, including devising lessons learned to prevent recurrence. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| CC7.5 | The entity identifies, develops, and implements activities to recover from identified security incidents. | Daily backups are performed and monitored to support recoverability of the production data. | Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data. | No exceptions noted. |
| | | The incident response plans are reviewed at least annually to confirm they provide an effective response to potential incidents. | Inspected the annual review of the incident response plans to determine that the incident response plans were reviewed at least annually to confirm they provided an effective response to potential incidents. | No exceptions noted. |

| CC7.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology establishes a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | Inspected the vulnerability management tool to determine Venn Technology established a process to identify security vulnerabilities, using reputable outside sources, and assign a risk ranking to newly discovered security vulnerabilities. | No exceptions noted. |
| | | The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems. | Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems. | No exceptions noted. |
| | | Venn Technology documents the scenarios and relevant impacts that may threaten Venn Technology's continuity, as well as the roles, responsibilities, and plans to manage those events effectively. | Inspected the business continuity plans to determine that Venn Technology documented the scenarios and relevant impacts that may threaten Venn Technology's continuity, as well as the roles, responsibilities, and plans to manage those events effectively. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |

## Common Criteria 8: Change Management

| CC8.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology uses a version control system to manage source code, documentation, release labelling, and other change management tasks. | Inspected the version control software to determine that Venn Technology used a version control system to manage source code, documentation, release labelling, and other change management tasks. | No exceptions noted. |
| | | When Venn Technology's application code changes, code reviews and tests are performed by someone other than the person who made the code change. | Inspected the systematic enforcement of peer reviews to determine that when Venn Technology's application code changes, code reviews and tests were performed by someone other than the person who made the code change. | No exceptions noted. |
| | | Only authorized Venn Technology personnel can deploy changes into production. | Inspected the access restrictions and roles to determine that only authorized Venn Technology personnel could deploy changes into production. | No exceptions noted. |
| | | Changes are automatically tested and approval flows are verified in the configured continuous integration/continuous deployment (CI/CD) software before they can be promoted to production. | Inspected the configuration of the CI/CD pipeline to determine that changes were automatically tested and approval flows verified in the configured continuous integration/continuous deployment (CI/CD) software before they could be promoted to production. | No exceptions noted. |
| | | Separate environments are used for testing and production for Venn Technology's Platform as a Service System. | Inspected the separation of environments to determine that separate environments were used for testing and production for Venn Technology's Platform as a Service System. | No exceptions noted. |

| CC8.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology has developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. | Inspected the policies and procedures to determine that Venn Technology had developed policies and procedures governing the system development life cycle, including documented policies for tracking, testing, approving, and validating changes. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |

## Common Criteria 9: Risk Mitigation

| CC9.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC9.1 | The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions. | Daily backups are performed and monitored to support recoverability of the production data. | Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data. | No exceptions noted. |
| | | Venn Technology utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | Inspected the multiple availability zones to determine that Venn Technology utilized multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | No exceptions noted. |
| | | Venn Technology follows a formal incident management process that includes logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | Inspected the incident handling for a sample of incidents to determine that Venn Technology followed a formal incident management process that included logging, classifying, and tracking incidents through to resolution with lessons learned devised to prevent recurrence. | No exceptions noted. |
| | | Restoration tests are conducted to check the integrity and completeness of back-up information on at least an annual basis. | Inspected the restoration tests to determine that restoration tests were conducted to check the integrity and completeness of back-up information on at least an annual basis. | No exceptions noted. |
| | | Venn Technology conducts annual business continuity and disaster recovery tests to ensure the response plans are effective. | Inspected the business continuity and disaster recovery tests to determine that Venn Technology conducted annual business continuity and disaster recovery tests to ensure the response plans were effective. | No exceptions noted. |

| CC9.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology maintains general liability insurance. | Inspected the liability insurance to determine that Venn Technology maintains general liability insurance. | No exceptions noted. |
| | | The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems. | Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems. | No exceptions noted. |
| | | Venn Technology documents the scenarios and relevant impacts that may threaten Venn Technology's continuity, as well as the roles, responsibilities, and plans to manage those events effectively. | Inspected the business continuity plans to determine that Venn Technology documented the scenarios and relevant impacts that may threaten Venn Technology's continuity, as well as the roles, responsibilities, and plans to manage those events effectively. | No exceptions noted. |
| | | Venn Technology documents the potential events, pre-planned response steps and communication requirements to ensure incidents are handled effectively. | Inspected the incident response plans to determine that Venn Technology documented the potential events, pre-planned response steps and communication requirements to ensure incidents were handled effectively. | No exceptions noted. |
| | | Venn Technology sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers. | Inspected the vendor management policy to determine that Venn Technology set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers. | No exceptions noted. |

| CC9.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| CC9.2 | The entity assesses and manages risks associated with vendors and business partners. | The vendor register includes material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | Inspected the vendor register to determine that the vendor register included material third-party software and service providers with tracking of the vendor agreements, risk ratings and vendor governance activities. | No exceptions noted. |
| | | Venn Technology performs security and compliance assessments of high-risk vendors. | Inspected the security and compliance review for a sample of high-risk vendors to determine that Venn Technology performed security and compliance assessments of high-risk vendors. | No exceptions noted. |
| | | Venn Technology establishes the scope of information assets and requirements for how those are tracked and managed accordingly. | Inspected the asset management policy to determine that Venn Technology established the scope of information assets and requirements for how those were tracked and managed accordingly. | No exceptions noted. |

### *Trust Services Criteria for the Availability Category*

| A1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| 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. | Venn Technology utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | Inspected the multiple availability zones to determine that Venn Technology utilized multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | No exceptions noted. |
| | | A load balancer automatically distributes incoming application traffic across multiple instances and availability zones. | Inspected the configured load balancer to determine that a load balancer automatically distributed incoming application traffic across multiple instances and availability zones. | No exceptions noted. |
| | | Auto-scaling configuration is used to automatically provision additional capacity when predefined thresholds are met. | Inspected the auto-scaling configuration to determine that auto-scaling configuration was used to automatically provision additional capacity when predefined thresholds were met. | No exceptions noted. |
| 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. | Daily backups are performed and monitored to support recoverability of the production data. | Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data. | No exceptions noted. |
| | | Venn Technology utilizes multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | Inspected the multiple availability zones to determine that Venn Technology utilized multiple availability zones to replicate production data across different zones to support the systems availability and recovery objectives. | No exceptions noted. |

| A1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology conducts annual business continuity and disaster recovery tests to ensure the response plans are effective. | Inspected the business continuity and disaster recovery tests to determine that Venn Technology conducted annual business continuity and disaster recovery tests to ensure the response plans were effective. | No exceptions noted. |
| | | The established disaster recovery plans outline roles, responsibilities, and detailed procedures for the recovery of critical systems. | Inspected the disaster recovery plans to determine that the established disaster recovery plans outlined roles, responsibilities, and detailed procedures for the recovery of critical systems. | No exceptions noted. |
| | | Venn Technology sets out the roles, responsibilities, and requirements for managing the risks associated with third-party providers. | Inspected the vendor management policy to determine that Venn Technology set out the roles, responsibilities, and requirements for managing the risks associated with third-party providers. | No exceptions noted. |
| | | Part of this criterion is the responsibility of the subservice organization. Refer to the Subservice Organizations section above for controls managed by the subservice organization. | | |
| A1.3 | The entity tests recovery plan procedures supporting system recovery to meet its objectives. | Daily backups are performed and monitored to support recoverability of the production data. | Inspected the daily backup configuration to determine that daily backups were performed and monitored to support recoverability of the production data. | No exceptions noted. |
| | | Restoration tests are conducted to check the integrity and completeness of back-up information on at least an annual basis. | Inspected the restoration tests to determine that restoration tests were conducted to check the integrity and completeness of back-up information on at least an annual basis. | No exceptions noted. |

| A1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology conducts annual business continuity and disaster recovery tests to ensure the response plans are effective. | Inspected the business continuity and disaster recovery tests to determine that Venn Technology conducted annual business continuity and disaster recovery tests to ensure the response plans were effective. | No exceptions noted. |

### *Trust Services Criteria for the Confidentiality Category*

| C1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| C1.1 | The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality. | Employment contracts are formed with Venn Technology employees including a non-disclosure agreement (NDA) for confidential information. | Inspected the employment contracts for a sample of new hires to determine that employment contracts were formed with Venn Technology employees including a non-disclosure agreement (NDA) for confidential information. | No exceptions noted. |
| | | Venn Technology defines the approach to test data to ensure the security and confidentiality of production data is maintained. | Inspected the software development policies to determine that Venn Technology defined the approach to test data to ensure the security and confidentiality of production data was maintained. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| | | Venn Technology requires role-based access control in line with the principle of least privilege where access rights are limited to the requirements of each role. | Inspected the access control policy to determine that Venn Technology required role-based access control in line with the principal of least privilege where access rights were limited to the requirements of each role. | No exceptions noted. |
| | | Venn Technology establishes the data types and retention periods of data collected and processed. | Inspected the data retention policies to determine that Venn Technology established the data types and retention periods of data collected and processed. | No exceptions noted. |

| C1.0 | Criteria | Control Activity | Test Applied by the Service Auditor | Test Results |
|---|---|---|---|---|
| | | Venn Technology establishes the method of data classification to ensure appropriate protections are applied based on its sensitivity. | Inspected the data classification policies to determine that Venn Technology established the method of data classification to ensure appropriate protections were applied based on its sensitivity. | No exceptions noted. |
| C1.2 | The entity disposes of confidential information to meet the entity's objectives related to confidentiality. | A formal offboarding process is followed to ensure that user devices, information assets, and system access for terminated employees has been revoked in a timely manner. | Inspected the terminations checklist for a sample of terminated employees to determine that a formal offboarding process was followed to ensure that user devices, information assets, and system access for terminated employees had been revoked in a timely manner. | No exceptions noted. |
| | | Venn Technology establishes the boundaries and requirements for how employees use Venn Technology's systems and information assets to protect against data leakage, malware, and security breaches. | Inspected the acceptable use policy to determine that Venn Technology established the boundaries and requirements for how employees used Venn Technology's systems and information assets to protect against data leakage, malware and security breaches. | No exceptions noted. |
| | | The disposal of sensitive information assets follows a defined process to ensure sensitive data is effectively erased before the safeguards over the information assets are removed. | Inspected the secure disposal policies and procedures to determine that the disposal of sensitive information assets followed a defined process to ensure sensitive data was effectively erased before the safeguards over the information assets were removed. | No exceptions noted. |

## *GUIDANCE REGARDING INFORMATION PROVIDED BY THE SERVICE AUDITOR*

AssuranceLab's examination of the controls of Venn Technology was limited to the related Agreed Criteria and control activities specified by the management of Venn Technology and did not encompass all aspects of Venn Technology's operations or operations at user entities. Our examination was performed in accordance with AT-C section 105: Concepts Common to All Attestation Engagements and AT-C section 205: Assertion-Based Examination Engagements.

Our examination of the control activities was performed using the following testing methods:

| TEST | DESCRIPTION |
|---|---|
| **Inquiry** | The service auditor made inquiries of service organization personnel. Inquiries were made to obtain information and representations from the client to determine that the client's knowledge of the control and corroborate policy or procedure information. |
| **Observation** | The service auditor observed application of the control activities by client personnel. |
| **Inspection** | The service auditor inspected among other items, source documents, reports, system configurations to determine performance of the specified control activity and in some instances the timeliness of the performance of control activities. |
| **Re-performance** | The service auditor independently executed procedures or controls that were originally performed by the service organization as part of the entity's internal control. |

In determining whether the report meets the criteria, the user auditor should perform the following procedures:

- Understand the aspects of the service organization's controls that may affect the service commitments and system requirements based on the Agreed Criteria
- Understand the infrastructure, software, procedures, and data that are designed, implemented, and operated by the service organization
- Determine whether the Agreed Criteria are relevant to the user entity's assertions
- Determine whether the service organization's controls are suitably designed to provide reasonable assurance that its service commitments and system were achieved based on the Agreed Criteria

## Office Locations


AUSTRALIA
Level 3/11 York Street
Sydney NSW 2000

UNITED STATES
1400 Lavaca Street, Suite 700
Austin, Texas 78701

EMEA
Block 2 Charlemont Street, Charlemont Row
Saint Kevin's, Dublin, D01 F6X6