Vena Solutions Inc.

System and Organization Controls 3 (SOC 3) report relevant to Security, Availability and Confidentiality for the Vena Cloud Platform Hosted on Azure for the period January 16, 2025 to April 30, 2025

Table of Contents

Deloitte.

Section 1 – Independent Service Auditor's Report

To: Management of Vena Solutions Inc. ("Vena" or "Vena Solutions" or the "Service Organization")

Scope

We have examined Vena's accompanying assertion titled "Assertion of Vena Management" (the "Assertion") that the controls within the Vena Cloud Platform Hosted on Azure (system) were effective throughout the period January 16, 2025 to April 30, 2025, to provide reasonable assurance that Vena's service commitments and system requirements would be achieved based on the trust services criteria relevant to 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,* in AICPA *Trust Services Criteria*.

The accompanying assertion and the Description of the Boundaries of the Vena Cloud Platform Hosted on Azure indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Vena, to achieve Vena's service commitments and system requirements based on the applicable trust services criteria. The Description of the Boundaries of the Vena Cloud Platform Hosted on Azure presents the complementary user entity controls assumed in the design of Vena's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Vena uses Microsoft Corporation ("Microsoft") and Amazon Web Services, Inc. ("Amazon" or "AWS"), collectively "subservice organizations", for hosting services. The accompanying management assertion and the Description of the Boundaries of the Vena Cloud Platform Hosted on Azure indicate that certain service commitments and system requirements based on the applicable trust services criteria can be met only if certain types of controls that management expects to be implemented at the subservice organizations are suitably designed, implemented, and operating effectively. The Description of the Boundaries of the Vena Cloud Platform Hosted on Azure presents the types of complementary subservice organization controls assumed in the design of Vena's controls. Our examination did not include the services provided by the subservice organizations, and we have not evaluated whether the controls management expects to be implemented at the subservice organizations have been implemented or whether such controls were suitably designed and operating effectively throughout the period January 16, 2025 to April 30, 2025.

Service Organization's Responsibilities

Management of Vena 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 Vena's service commitments and system requirements were achieved. Management of Vena has also provided the accompanying assertion in Section 2 titled, "Assertion of Vena Management" about the effectiveness of controls within the system. When preparing its assertion, Vena is responsible for selecting, and identifying in its assertion, the applicable trust service criteria and for having a reasonable basis for its assertion by performing an assessment of the effectiveness of the controls within the system.

Deloitte.

Service Auditor's Responsibilities

Our responsibility is to express an opinion, based on our examination, on whether management's assertion that controls within the system were effective throughout the period to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination included:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements.
- Assessing the risks that controls were not effective to achieve Vena's service commitments and system requirements based on the applicable trust services criteria.
- Performing procedures to obtain evidence about whether controls within the system were effective to achieve Vena's service commitments and system requirements based on the applicable trust services criteria.

Our examination also included performing such other procedures as we considered necessary in the circumstances.

Service Auditor's Independence and Quality Control

We have complied with the relevant rules of professional conduct / code of ethics applicable to the practice of public accounting and related to assurance engagements, issued by various professional accounting bodies, which are founded on fundamental principles of integrity, objectivity, professional competence and due care, confidentiality and professional behaviour.

The firm applies Canadian Standard on Quality Management 1, *Quality Management for Firms that Perform Audits or Reviews of Financial Statements, or Other Assurance or Related Services Engagements*, which requires the firm to design, implement and operate a system of quality management, including policies or procedures regarding compliance with ethical requirements, professional standards and applicable legal and regulatory requirements.

Inherent Limitations

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls.

Because of their nature, controls may not always operate effectively to provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Deloitte.

Emphasis of a Matter – No Live Customers for a Portion of the Reporting Period

As indicated in Vena's Description, the Vena Cloud Platform Hosted on Azure went live on November 1, 2024; however, no customers were onboarded as of January 31, 2025; therefore, we did not perform any tests of the design, implementation or operating effectiveness of those controls related to: (a) notification to customers for scheduled maintenance, (b) back-up of customer data, and (c) deletion of customer tenants and archives, and accordingly, we do not express an opinion on the design, implementation or operating effectiveness of these controls to achieve the service commitments and system requirements based on the applicable trust services criteria from January 16, 2025 to January 31, 2025.

Opinion

In our opinion, apart from the matter referred to in the preceding paragraph, management's assertion that the controls within the Vena Cloud Platform Hosted on Azure were effective throughout the period January 16, 2025 to April 30, 2025, if complementary subservice and user entity controls contemplated in the design of Vena's controls operated effectively, to provide reasonable assurance that Vena's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

Deloitte LLP

Chartered Professional Accountants
Toronto, Canada
June 17, 2025

Section 2 – Assertion of Vena Management

We are responsible for designing, implementing, operating, and maintaining effective controls within Vena Solutions Inc. ("Vena" or "Vena Solutions" or the "Service Organization") related to the Vena Cloud Platform Hosted on Azure ("VHOA") throughout the period January 16, 2025 to April 30, 2025, to provide reasonable assurance that Vena's service commitments and system requirements relevant to security, availability and confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period January 16, 2025 to April 30, 2025, to provide reasonable assurance that Vena's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability and confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* in AICPA, *Trust Services Criteria*. Vena's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Sections 3 and 4.

Vena uses Microsoft Corporation ("Microsoft") and Amazon Web Services, Inc. ("Amazon" or "AWS"), collectively "subservice organizations", for hosting services. This assertion and the Description of the Boundaries of the Vena Cloud Platform Hosted on Azure indicate that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Vena, to achieve Vena's service commitments and system requirements related to the delivery of its services as it relates to the Vena Cloud Platform Hosted on Azure based on the applicable trust services criteria. The accompanying Description of the Boundaries of the Vena Cloud Platform Hosted on Azure presents the types of complementary subservice organization controls assumed in the design of Vena's controls. The actual controls at the subservice organizations are not disclosed.

This assertion and the Description of the Boundaries of the Vena Cloud Platform Hosted on Azure indicate that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Vena, to achieve Vena's service commitments and system requirements related to the delivery of its services as it relates to the Vena Cloud Platform Hosted on Azure based on the applicable trust services criteria. The accompanying Description of the Boundaries of the Vena Cloud Platform Hosted on Azure presents the complementary user entity controls assumed in the design of Vena's controls.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of these inherent limitations, a service organization may achieve reasonable, but not absolute, assurance that its service commitments and system requirements are achieved.

We assert that, apart from the matter described in the following paragraph, the controls within the system were effective throughout the period January 16, 2025 to April 30, 2025, to provide reasonable assurance that Vena's service commitments and system requirements were achieved based on the applicable trust services criteria.

As indicated in our Description, the Vena Cloud Platform Hosted on Azure went live on November 1, 2024; however, no customers were onboarded as of January 31, 2025; therefore, no tests of the design, implementation or operating effectiveness related to controls over: (a) notification to customers for scheduled maintenance, (b) back-up of customer data, and (c) deletion of customer tenants and archives, were performed from January 16, 2025 to January 31, 2025.

Vena Solutions Inc.
June 17, 2025

Section 3 – Description of the Boundaries of the Vena Cloud Platform Hosted on Azure

3.1 Company Overview

Vena was founded in 2011 in Toronto, Canada by an experienced team who spent years at leading software companies, including Clarity and IBM, developing and implementing corporate performance management (CPM) solutions that replaced traditional spreadsheet-based planning processes.

Vena is a CPM solution, which provides cost-effective, user-friendly and easy to implement Cloud Financial Planning & Analysis (FP&A) software that ties the power and flexibility of Excel to a secure, centrally managed application.

Service offerings provided by Vena (comprising of Vena Solutions Inc. and its affiliates) offer a multi-tenant SaaS (Software-as-a-Service) solutions built on Microsoft Azure and Amazon Web Services. Vena's services include the storage and processing of a company's confidential financial, employee and/or operational information and identity management for users of the system.

3.2 Overview of the Vena Cloud Platform Hosted on Azure

The Vena Cloud Platform (also referred to as Growth Engine Platform) is a powerful corporate performance management software solution that helps companies budget and plan to grow their businesses. The major client features that make up the platform are:

- Online analytical processing (OLAP) Data Model: Customers can store large volumes of data for processing and multi-dimensional analysis.
- Microsoft Excel Add-In for Windows: Allows users to leverage the ease of use and flexibility of Excel to read and write data from their OLAP models for the purpose of budgeting and reporting.
- Microsoft Excel Add-In for Microsoft 365: Allows users to leverage the ease of use and flexibility of Excel to read and write data from their OLAP models for the purpose of budgeting and reporting. Built on the Microsoft 365 App Store for use on platforms.
- Workflow Engine: Build and automate planning cycles that enable finance teams to scale budgeting and reporting processes for up to thousands of users.
- Calculations Engine: Used for writing advanced calculation scripts to transform and aggregate data stored in OLAP data model intersections.
- Integrations: Enable the flow of transactions from the customers' source systems into Vena for calculating "actuals" and financial statements.

- Collaboration and Task Management: Users can add comments, be assigned tasks in a workflow, or review embedded documentation all in the service of scaling the planning process across the customers' budget stakeholders.

- Pre-Configured Solutions: Vertical and horizontal pre-built data models, templates, and workflows for specific planning types that help get a customer up and running faster.

- User Management and Security: Role-based security that dictates a user's access to both application features and data sets.

Vena's Growth Engine Platform combined with Vena's Pre-Configured Solutions offer customers a "Complete Planning Solution" for the following applications:

- Revenue Planning
- Forecasting
- Operational Planning
- Scenario Modeling
- Financial Reporting
- Dashboarding and Analytics
- Financial Consolidations
- Financial Close Management

Vena Insights is Vena's intelligent reporting and analytics solution which leverages the power of Microsoft's Power BI ecosystem to drive strategic insights through a fully productized user interface. Participating customers can use and customize advanced machine learning models to focus analysis on the most relevant business drivers for their organizations. Power BI Embedded Analytics is woven into the Vena interface for the most intuitive experience.

This direct integration with the Vena Cloud Platform instantly applies best practices, multi-dimensional modeling, and scenario analysis capabilities so that participating customers can quickly maximize Power BI's AI-enabled insights and analysis across their entire business. To accomplish this, Vena leverages integration between the Vena application and the Microsoft Power BI Service, which is the SaaS version of Power BI hosted in Microsoft Azure.

Vena Copilot is an AI-powered assistant designed for FP&A, leveraging Microsoft Azure AI Services to enhance productivity by performing tasks such as data gathering, report generation, trend analysis, and forecast optimization. For participating customers, it enables FP&A teams to interact using a conversational interface, streamlining complex tasks with natural language prompts and existing organizational data sets.

The Vena Cloud Platform Hosted on Azure went live on November 1, 2024; however, no customers were onboarded as of January 31, 2025. This report is intended to provide information sufficient to understand the relevant aspects of Vena's control environment for the Vena Cloud Platform Hosted on Azure throughout the period January 16, 2025 to April 30, 2025, specifically as it relates to the security, availability and confidentiality trust service criteria.

The scope of this report does not include:

- Processes and controls of other solutions offered by Vena;
- External processes and controls that are performed by user entities of the system;
- Controls related to (a) notification to customers for scheduled maintenance, (b) back-up of customer data, and (c) deletion of customer tenants and archives for the period January 16, 2025 to January 31, 2025, as no customers were onboarded into the Vena Cloud Platform Hosted on Azure as of January 31, 2025; and
- Controls at various organizations that Vena has made arrangements with to facilitate the delivery of services, such as Microsoft Corporation ("Microsoft") and Amazon Web Services, Inc. ("Amazon" or "AWS").

3.3 Components of the System used to provide services

3.3.1 Infrastructure

Infrastructure consists of the physical structures, IT, and other hardware (for example, facilities, computers, equipment, mobile devices, and telecommunications networks). The Vena Cloud Platform Production Network (defined as the environment in which the Vena Cloud Platform is located and made available to authorized users) is hosted in geographically distributed Microsoft Azure data centres. These data centres consist of firewalls, switches, load balancers, routers, servers, and databases that house or transmit Service Data, Subscriber Data, application code, as well as related system monitoring utilities. Azure Blob Storage contain customer uploaded files, database backups and logs while Azure VM instances are used to provide processing of subsets of Service Data. Service Data refers to transaction streams, files, data stores, tables, and output used or processed by the system. Subscriber Data is defined as any information that is created, inputted, submitted, posted, transmitted, stored, or displayed by customers, customer agents, and customers' customers – who are also referred to as Vena Cloud Platform end-users.

Vena utilizes globally distributed Vena hubs currently located in the United States (US), Canada, and the European Union (EU), where infrastructure is hosted. This provides customers with an option to host their Vena Cloud Platform instance in a preferred geographic location. Each Vena hub has Vena service infrastructure deployed across multiple availability zones (physical Microsoft Azure data centers), utilizing a primary operating region and a paired DR region within the same geography.

Vena hosts its infrastructure within Microsoft Azure data center facilities. Microsoft Azure data centers are designed to host mission critical servers and computer systems, with fully redundant subsystems (cooling, power, network links, storage) and compartmentalized security zones controlled by biometric or other access control methods. Microsoft Azure houses systems in secure, hardened facilities that employ onsite security guards, video surveillance, and biometric/keycard-based access.

<u>Database Architecture – Redundancy and Separability</u>

Each Vena hub contains several database types. The primary datastore used to store financial information – MongoDB – is configured in a highly-available configuration consisting of three instances per cluster. Each cluster consists of one instance assuming a primary (write/read) role and the other two instances assuming a secondary (read-only) role that continuously replicate the primary instance's data. If the instance holding the primary role unexpectedly encounters a problem, one of the secondary instances immediately is promoted to the new primary role. This automated system of fault tolerance and database failover reduces the risk of downtime. Customer tenants (databases) within a Vena hub are sharded across multiple MongoDB clusters.

Other databases within Vena's platform are configured with similar forms of redundancy. Azure Database for MySQL is used for storing the product's relational (SQL-accessed) data. Azure Database for MySQL is

configured in a highly-available configuration so that if the current underlying instance is disrupted, a new instance with an up-to-date copy of database data comes online without impacting the Vena application. Azure Data Explorer (ADX) (used for Vena's financial audit table data) separates storage and compute resources. Persistent data resides in Azure Blob Storage, while compute resources duplicate writes across multiple nodes so that in the event of an instance-level failure, another instance can continue to serve the data. Lastly, Azure SQL Database (ASD), a full PaaS service, is leveraged for Vena's staging and VenaTables functionality.

Customer tenant databases are segregated from one another.

3.3.2 Software

Software consists of the application programs and IT system software that supports application programs (operating systems, middleware, and utilities). Vena's software stack consists of Linux instances running Nginx HTTP server, databases supported by MongoDB, Azure Database for MySQL, Azure SQL Database and Azure Data Explorer, messaging supported by RabbitMQ, and distributed locking control supported by Apache Zookeeper. Vena leverages a mix of Azure VM images and container images containing the latest Linux distribution image. Services are hosted via of Azure VMSS (Virtual Machine Scale Sets) and Azure Container Apps (ACA) services. The images used are updated weekly to help ensure they include the latest patches and updates. These machine images are also used to update and manage a standard build image for new server deployments. Ansible, the configuration management tool, has "playbooks" that are used to actively manage the infrastructure configuration across servers. Java and JavaScript are the primary programming languages used for developing the Vena Cloud Platform, while Python, Ansible and Terraform are used within the infrastructure codebase.

3.3.3 People

The following Vena personnel are involved in the governance, operation, and use of the system:

- Product and Technology – Responsible for the design, development, testing, deployment, and maintenance of new code for Vena production applications. Consists of multiple teams with specific assignments including Architecture, Quality Assurance, and Product Development.

- SaaS Technology and Operations (STO) – A subset of the Product and Technology Team. Responsible for overall platform uptime, ITIL process enforcement and core infrastructure configuration changes. Additionally, responsible for granting logical access to the systems within the Vena Production Network, performing semi-annual reviews of access to those systems, and revoking logical access rights upon user termination. Azure manages the distributed denial-of-service (DDoS) protections for layer 3 and layer 4 network layers. STO is responsible for overall system availability, including establishing best practices for system availability, resiliency, system logging and monitoring, backup and recovery, and capacity planning. STO works closely with the Corporate Security and Data Privacy Team to remediate discovered system vulnerabilities. STO is also responsible for monitoring the availability and capacity of infrastructure and relevant services, and to track significant issues to resolution using the incident management process.

- Enterprise Information Technology (EIT) – Responsible for managing corporate computing devices (laptops/endpoints), business applications, supporting toolsets, and employee and contractor identities. IT grants access to SaaS applications and to systems within the corporate network and manages and terminates access when applicable.

- Corporate Security and Data Privacy – Responsible for overall security governance, security risk management, security awareness, incident response and crisis management, and the monitoring and testing of security control effectiveness across Vena.

- Human Resources – Responsible for onboarding new personnel, defining the role/position of new hires, performing background checks, and facilitating the employee termination process.

- Facilities – Responsible for managing physical security and granting physical access to Vena corporate offices.

- Customer Experience – Responsible for managing customer interactions via email, chat, social media and over the phone. The team fields and resolves customer inquiries and issues regarding Vena plans, training, and technical issues related to the software. They are also responsible for communicating information to customers regarding new issues and/or developments, system enhancements, new product features and updates, security incidents, and other relevant information. Additionally, our Professional Services group within our Customer Experience department works with our customers to implement the software.

- Legal – Responsible for collaborating with internal stakeholders to draft and negotiate contracts with third parties (e.g., customers, partners, suppliers, etc.) in accordance with corporate contracting standards and risk appetite, and facilitating review of information security and privacy issues.

3.3.4 Data

The customer defines and controls the Subscriber Data they load and store in the Vena Production Network via the Vena Cloud Platform. Subscriber Data is loaded into the environment and accessed remotely from customer systems via the Internet. Subscriber Data is backed up periodically, any issues in backup are monitored through automated notifications and tracked through to resolution. Subscriber Data is retained as contractually mandated by the Master Services Agreement.

Except as otherwise required pursuant to applicable contractual arrangements or to comply with legal obligations, (a) Subscriber Data is purged from the Vena Production Network within 90 days of end of quarter of customer churn, and (b) an archive of the snapshot of Subscriber Data is taken prior to deletion, which is retained for 180 days prior to deletion. Former customers may also request to delete the archived snapshot of Subscriber Data, which is actioned on by Vena in a timely manner.

Vena also stores user credentials, namely usernames and passwords used to authenticate access to the Vena Cloud Platform. Password data is "salted" (mixed with random data) and hashed using a cross-platform hashing utility. The hash and salt identifier, and not the password itself, is what is stored in the database. Password hashing is managed in the application, and to verify that the password is correct, Vena compares the result of hashing the user-entered password against the stored one-way hash. This means that user passwords are not written to the database in a human readable format. User passwords and other authentication credentials are also filtered out from logs, prior to writing the logs to disk.

Authentication may also be done via Single Sign-On (SSO) using Security Assertion Markup Language (SAML) if configured at the customer level. In this case, no password data is stored on Vena systems as authentication is done through the third party SSO provider.

3.3.5 Processes and Procedures

Processes include the automated and manual procedures involved in the operation of the Vena Growth Engine Platform. Procedures are developed and documented by the respective teams for a variety of processes, including those relating to Operations, Security, Product, and IT. Vena has several policies, which have associated procedures supporting them. These procedures are prepared in alignment with the applicable policies and are updated and approved as necessary for changes in the business but are reviewed no less than annually.

3.4 Changes to the System During the Period

There were no changes to the Vena Cloud Platform Hosted on Azure made available to user entities of the system that are likely to affect intended report users' understanding of how the Vena Cloud Platform Hosted on Azure is used to provide the service during the period January 16, 2025 to April 30, 2025.

3.5 System Incidents

There were no system incidents that impacted the overall achievement of our service commitments and system requirements based on the trust services criteria during the period January 16, 2025 to April 30, 2025.

3.6 Complementary Controls Considerations

The following section outlines the complementary user entity and subservice organization control considerations that would be relevant as they relate to the controls at Vena. These control considerations were not subject to examination by the Service Auditor.

3.6.1 Complementary User Entity Control (CUECs)

The Vena Cloud Platform Hosted on Azure was designed with the assumption that certain controls would be implemented by user entities. These controls should be in operation at user entities to complement Vena's controls. The user entity controls presented below should not be regarded as a comprehensive list of all controls that should be employed by user entities. User entities of the Vena Cloud Platform Hosted on Azure should maintain controls to provide reasonable assurance that:

#	Complementary User Entity Control
1	User entities must meet requirements and obligations as outlined in their individual agreements with Vena.
2	User entities are responsible for informing Vena of any changes to the requirements that may impact the services provided.
3	User entities are responsible for reporting problems of the Vena Cloud Platform Hosted on Azure to Vena in a timely manner.
4	User entities are responsible for ensuring that Vena Cloud Platform Hosted on Azure users attend training to gain proficiency in using the application as related to their job functions.
5	User entities are responsible for the setup and maintenance of client users' security profiles, user accounts, passwords and password policies within the Vena Cloud Platform Hosted on Azure.
6	User entities are responsible for having formal termination procedures in place to ensure that logical access is revoked in a timely manner.
7	User entities are responsible to provide and revoke access to the support feature in the Vena Cloud Platform Hosted on Azure.
8	User entities are responsible for reviewing user access lists to ensure that only authorized and appropriate users have access to the Vena Cloud Platform Hosted on Azure.

#	Complementary User Entity Control
9	User entities are responsible for responding to and reacting to potential security violations or misuse of their tenant on the Vena Cloud Platform Hosted on Azure.
10	User entities are responsible for selection, use, compatibility and maintenance of hardware and software to use the Vena Cloud Platform Hosted on Azure.
11	User entities are responsible for installation, operation and maintenance of hardware and software used to transmit and receive electronic information to and from Vena.
12	User entities are responsible for the configuration of their tenant on the Vena Cloud Platform Hosted on Azure.
13	User entities are responsible to explicitly request deletion of archived snapshot(s) of their tenant data.
14	User entities are responsible for configuring Vena Support User (VSU) access in their tenant, per their business requirements.
15	User entities are responsible to check the online Vena service status page for updates to the platform.

3.6.2 Complementary Subservice Organization Controls (CSOCs)

Vena uses subservice organizations in the delivery of its services. The description indicates that complementary subservice organization controls that are suitably designed and implemented along with controls at Vena, are required to achieve Vena's service commitments and system requirements based on applicable criteria.

The table below summarizes the controls that Vena expects the subservice organizations to perform, and the corresponding trust services criteria intended to be met. The Service Auditor's examination did not extend to the controls of the subservice organizations and the Service Auditor has not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Subservice provider(s)	Illustrative controls expected to be implemented by the subservice organizations
Microsoft Corporation	• Microsoft enables customers to articulate who has access to Microsoft services and resources (if resource-level permissions are applicable to the service) that they own. Microsoft prevents customers from accessing resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified Microsoft service or resource (if resource-level permissions are applicable to the service). • Only authorized Microsoft personnel have physical access to Vena's systems housed at Microsoft's facilities. • Security personnel at Microsoft identifies and monitors individuals' physical access. • Users' physical access to the data centre is periodically reviewed and validated by Microsoft. • All production media is securely decommissioned and physically destroyed prior to leaving secure zones. • Microsoft provides customers the ability to delete their content. Once successfully removed, the data is rendered unreadable. • Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. • Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. • Network communications within a virtual network are isolated from each other. • Roles and responsibilities for Azure Key Vault cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities changes.

Subservice provider(s)	Illustrative controls expected to be implemented by the subservice organizations
	• The key provided by Azure Key Vault to integrated services is encrypted with a 256-bit AES key. • Data is backed up and retained as configured, and the network is monitored for security requirements to prevent unauthorized access.Security breaches at Microsoft are documented, investigated, and resolved. • Vena is notified of breaches or incidents that may impact their systems housed at Microsoft. • Security and alarm systems are used to secure Microsoft's facilities. • Microsoft applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Microsoft guidelines and tailored to the specifics of each Microsoft service. • Microsoft uses data masking and anonymization techniques to protect sensitive information in non-production environments such as development and testing. • Microsoft requires all employees, contractors, and third-party service providers to sign confidentiality agreements to protect sensitive information. • Microsoft develops and maintains comprehensive disaster recovery and business continuity plans to ensure that services can be quickly restored in the event of a disruption. They regularly test and update these plans to ensure their effectiveness. • Microsoft continuously monitors system performance and resource utilization to identify potential bottlenecks and capacity issues. They conduct capacity planning to ensure that the infrastructure can handle increased loads and future growth. • Microsoft establishes SLAs with clear uptime and response time commitments to provide customers with assurance regarding the availability of the service. They monitor and report on SLA performance to ensure compliance and identify areas for improvement.
Amazon Web Services, Inc.	• AWS enables customers to articulate who has access to AWS services and resources (if resource-level permissions are applicable to the service) that they own. AWS prevents customers from accessing AWS resources that are not assigned to them via access permissions. Content is only returned to individuals authorized to access the specified AWS service or resource (if resource-level permissions are applicable to the service). • 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. • Amazon-owned data centers are protected by fire detection and suppression systems. • 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.

Subservice provider(s)	Illustrative controls expected to be implemented by the subservice organizations
	• AWS production media is securely decommissioned and physically destroyed prior to leaving AWS Secure Zones. • Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents. • Firewall devices are configured to restrict access to the computing environment and enforce boundaries of computing clusters. • VPC-Specific – Network communications within a VPC are isolated from network communications within other VPCs. • KMS-Specific – Roles and responsibilities for KMS cryptographic custodians are formally documented and agreed to by those individuals when they assume the role or when responsibilities changes. • KMS-Specific – The key provided by KMS to integrated services is a 256-bit key and is encrypted with a 256-bit AES master key unique to the customer's AWS account. • Data is backed up and retained as configured, and the network is monitored for security requirements to prevent unauthorized access. • AWS provides publicly available mechanisms for customers to contact AWS to report security events and publishes information including a system description and security and compliance information addressing AWS commitments and responsibilities. • AWS applies a systematic approach to managing change to ensure changes to customer-impacting aspects of a service are reviewed, tested and approved. Change management standards are based on Amazon guidelines and tailored to the specifics of each AWS service. • Monitoring and alarming are configured to identify and notify operational and management personnel of incidents when early warning thresholds are crossed on key operational metrics. • AWS uses data masking and anonymization techniques to protect sensitive information in non-production environments such as development and testing. • AWS requires all employees, contractors, and third-party service providers to sign confidentiality agreements to protect sensitive information. • AWS develops and maintains comprehensive disaster recovery and business continuity plans to ensure that services can be quickly restored in the event of a disruption. They regularly test and update these plans to ensure their effectiveness. • AWS continuously monitors system performance and resource utilization to identify potential bottlenecks and capacity issues. They conduct capacity planning to ensure that the infrastructure can handle increased loads and future growth. • AWS establishes SLAs with clear uptime and response time commitments to provide customers with assurance regarding the availability of the service. They monitor and report on SLA performance to ensure compliance and identify areas for improvement.

Section 4 – Principal Service Commitments and System Requirements

Vena makes service commitments to its customers and has established system requirements as part of the Vena Cloud Platform Hosted on Azure. Some of these commitments are key to the performance of the service and relate to applicable trust services criteria. Vena is responsible for its service commitments and system requirements and for designing, implementing, and operating effective controls within the Vena Cloud Platform Hosted on Azure to provide reasonable assurance that Vena's service commitments and system requirements are achieved.

Systems are designed to protect against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability and integrity of information or systems. This includes the protection of

i. information during its collection or creation, use, processing, transmission, and storage; and

ii. systems that use electronic information to process, transmit or transfer, and store information to enable the achievement of Vena's service commitments and system requirements. Controls over security, confidentiality and availability are designed to 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.

Controls are designed to ensure that information and systems are available for operation and use to meet Vena's objectives. Management's controls around the Vena Cloud Platform Hosted on Azure support accessibility for operation, monitoring and maintenance. They are designed to ensure that information used by Vena's systems, as well as products or services provided to its customers remains accessible.

Controls are designed to ensure that information designated as confidential is protected to meet Vena's objectives. Management's controls around the Vena Cloud Platform Hosted on Azure are designed to ensure that the entity can protect information designated as confidential from its collection or creation through its final disposition and removal from entity's control. These controls are designed to ensure that confidential data is protected from access, use, and retention and its disclosure is restricted to defined parties.

Service commitments to Vena's customers are documented and communicated in Maintenance and Support Agreements, which form part of Vena's standard customer contracts. Security, confidentiality and availability procedures and commitments, including customer obligations, are communicated through customer contracts and/or the Customer Experience Team.

