Insight Assurance

SOC 2 | ISO 27001 | PCI | HIPAA

System and Organization Controls Report (SOC 2® Type 1)

Report on Fraxion Spend Management LLC's Description of Its Fraxion's Spend Management Services system and on the Suitability of the Design of Its Controls Relevant to Security as of November 1, 2024

fraxion

TABLE OF CONTENTS

SECTION 1: INDEPENDENT SERVICE AUDITOR'S REPORT

Insight Assurance
SOC 2 | ISO 27001 | PCI | HIPAA

INDEPENDENT SERVICE AUDITOR'S REPORT

To: Fraxion Spend Management LLC

Scope

We have examined Fraxion Spend Management LLC's ("Fraxion" or "the Service Organization") accompanying description of its Fraxion's Spend Management Services system found in Section 3 titled "Fraxion Spend Management LLC's description of its Fraxion's Spend Management Services system" as of November 1, 2024 ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria) and the suitability of the design of controls stated in the description as of November 1, 2024, to provide reasonable assurance that Fraxion's service commitments and system requirements would be achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria.*

Fraxion uses Microsoft Azure (Azure) to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fraxion, to achieve Fraxion's service commitments and system requirements based on the applicable trust services criteria. The description presents Fraxion's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Fraxion's controls. The description does not disclose the actual controls at the subservice organization. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that certain complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fraxion, to achieve Fraxion's service commitments and system requirements based on the applicable trust services criteria. The description presents Fraxion's controls, the applicable trust services criteria and the complementary user entity controls assumed in the design of Fraxion'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.

Service Organization's Responsibilities

Fraxion is responsible for its service commitments and system requirements and designing, implementing, and operating effective controls within the system to provide reasonable assurance that Fraxion's service commitments and system requirements would be achieved. In Section 2, Fraxion has provided the accompanying assertion titled "Fraxion Spend Management LLC's Management Assertion" (assertion) about the description and the suitability of the design of controls stated therein. Fraxion is also responsible for preparing the description and assertion, including the completeness, accuracy, and method of presentation of the description and assertion; providing the services covered by the description; selecting the applicable trust services criteria, and stating the related controls in the description; and identifying the risks that threaten the achievement of the service organization's service commitments and system requirements.

Service Auditor's Responsibilities

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

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

An examination of a description of a service organization's system and the suitability of the design of controls involves—

- obtaining an understanding of the system and the service organization's service commitments and system requirements.
- assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed.
- performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria.
- performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization would achieve its service commitments and system requirements based on the applicable trust services criteria.
- evaluating the overall presentation of the description.

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual report users may consider important to meet their informational needs. There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. The projection to the future of any conclusions about the suitability of the design of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, in all material respects,

- the description presents Fraxion's Spend Management Services system that was designed and implemented as of November 1, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of November 1, 2024, to provide reasonable assurance that Fraxion's service commitments and system requirements would be achieved based on the applicable trust services criteria if its controls operated effectively as of that date and if the subservice organization and user entities applied the complementary controls assumed in the design of Fraxion's controls as of that date.

Restricted Use

This report is intended solely for the information and use of Fraxion, user entities of Fraxion's Spend Management Services system as of November 1, 2024, business partners of Fraxion subject to risks arising from interactions with the Fraxion's Spend Management Services 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 organization, 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 applicable trust services criteria.
- The risks that may threaten the achievement of the service organization's service commitments and system requirements and how controls address those risks.

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

Insight Assurance LLC

Tampa, Florida
January 30, 2025

SECTION 2: FRAXION SPEND MANAGEMENT LLC'S MANAGEMENT ASSERTION

fraxion

FRAXION SPEND MANAGEMENT LLC'S MANAGEMENT ASSERTION

We have prepared the description of Fraxion Spend Management LLC's ('Fraxion' or 'the Service Organization') Fraxion's Spend Management Services system entitled "Fraxion Spend Management LLC's description of its Fraxion's Spend Management Services system" as of November 1, 2024 ("description") based on the criteria for a description of a service organization's system set forth in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report (With Revised Implementation Guidance—2022)* in AICPA, *Description Criteria*, (description criteria). The description is intended to provide report users with information about the Fraxion's Spend Management Services system that may be useful when assessing the risks arising from interactions with Fraxion's system, particularly information about system controls that Fraxion has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA, *Trust Services Criteria*.

Fraxion uses Azure to provide hosting services. The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Fraxion, to achieve Fraxion's service commitments and system requirements based on the applicable trust services criteria. The description presents Fraxion's controls, the applicable trust services criteria and the types of complementary subservice organization controls assumed in the design of Fraxion's controls. The description does not disclose the actual controls at the subservice organization.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Fraxion, to achieve Fraxion's service commitments and system requirements based on the applicable trust services criteria. The description presents the subservice organization controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Fraxion's controls.

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

- the description presents Fraxion's Spend Management Services system that was designed and implemented as of November 1, 2024, in accordance with the description criteria.
- the controls stated in the description were suitably designed as of November 1, 2024, to provide reasonable assurance that Fraxion's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively as of that date, and if the subservice organization and user entities applied the complementary controls assumed in the design of the Fraxion's controls as of that date.

Fraxion Spend Management LLC
January 30, 2025

SECTION 3: FRAXION SPEND MANAGEMENT LLC'S DESCRIPTION OF ITS FRAXION'S SPEND MANAGEMENT SERVICES SYSTEM

FRAXION SPEND MANAGEMENT LLC'S DESCRIPTION OF ITS FRAXION'S SPEND MANAGEMENT SERVICES SYSTEM

Company Background

Fraxion Spend Management LLC ("Fraxion" or "the company") is a privately held company established in October 2016. The company offers Spend Management Services. Fraxion is headquartered in Seattle, Washington and Cape Town, South Africa.

Description of Services Overview

Fraxion provides companies with a spending management solution that offers. The cloud-based platform is designed to simplify procurement, streamline approval processes, and enhance compliance, all while delivering measurable savings. The company offers the following:

- Spend Management Software.
- Procurement Automation.
- Budget Control.
- Compliance and Audit Readiness.
- Cloud-Based Accessibility.

PRINCIPAL SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Fraxion designs its processes and procedures related to Fraxion's Spend Management Services system to meet its objectives. Those objectives are based on the service commitments that Fraxion makes to user entities, the laws, and regulations that govern the provision of the services, and the financial, operational, and compliance requirements that Fraxion has established for the services.

Security commitments to user entities are documented and communicated in Privacy Policy and Terms of Service (TOS).

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

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

Fraxion establishes operational requirements that support the achievement of security, relevant laws and regulations, and other system requirements. Such requirements are communicated in system policies and procedures, system design documentation, and agreements with customers. Information security policies define an organization-wide approach to how systems and data are protected. These include policies around how the service is designed and developed, how the system is operated, how the internal business systems and networks are managed, and how employees are hired and trained. In addition, how to carry out specific manual and automated processes required in the operation and development of the System.

COMPONENTS OF THE SYSTEM

The System description is comprised of the following components:

- ***Infrastructure*** – The collection of physical or virtual resources that supports an overall IT environment, including the physical environment and related structures, IT and hardware (for example, facilities, servers, storage, environmental monitoring equipment, data storage devices and media, mobile devices, and internal networks and connected external telecommunications networks) that the service organization used to provide the services.
- ***Software*** – The application programs and IT system software that supports application programs (operating systems, middleware, and utilities), the types of databases used, the nature of external facing web applications, and the nature of applications developed in-house, including details about whether the applications in use are mobile applications or desktop or laptop applications.
- ***People*** – The personnel involved in the governance, operation, security, and use of a system (business unit personnel, developers, operators, user entity personnel, vendor personnel, and managers).
- ***Data*** – The types of data used by the system, such as transaction streams, files, databases, tables, and output used or processed by the system.
- ***Procedures*** – The automated and manual procedures related to the services provided, including, as appropriate, procedures by which service activities are initiated, authorized, performed, and delivered, and reports and other information prepared.

INFRASTRUCTURE

Fraxion maintains a system inventory that includes virtual machines, computers (desktops and laptops), and networking devices (switches and routers). The inventory documents device name, device type, vendor function, OS, location, and notes. The in-scope Fraxion infrastructure components are shown in the table below:

Primary Infrastructure		
Hardware	**Type**	**Purpose**
SonicWall TZ 400	SonicWall	Used as a site-to-site VPN gateway, providing a secure, encrypted connection between their on-premises network and Azure cloud network, ensuring all data transmitted is protected from potential interception. Fraxion use the device for its security features, including

Primary Infrastructure		
Hardware	**Type**	**Purpose**
		deep packet inspection firewall, intrusion prevention system (IPS), and application control, to protect company's network from unauthorized access, malware, and other security threats. When working from home, Fraxion use the Azure VPN client, which authenticates with Multi-Factor Authentication (MFA).
D-Link DGS-1210-28 (Switch)	Azure	Fraxion use the D-Link DGS-1210-28 switch exclusively to connect Wi-Fi access points, ensuring reliable network connectivity for wireless devices (Laptops). Servers hosted in Azure - Only accessible only via VPN for enhanced security.
PRODNETDC01	Azure	Domain Controller in West US 3, handling core directory services for production.
PRODNETDC02	Azure	Domain Controller in South African North, providing redundancy and directory services for production.
PRODNETDC1	Azure	Domain Controller in West US 2, supporting production directory services for the region.
CERTISSUER	Azure	Certificate management server responsible for issuing and managing SSL/TLS certificates.
TESTDC01	Azure	Domain Controller in West US 3 used for testing patch deployment and configuration changes before production implementation.
WOODFIREDPIZZA	Azure	Server syncing Active Directory objects to Entra ID for hybrid identity management.
PRODWEBSERVER	Azure	Web server hosting internal password management software and the FogBugz software used by the sales team.
ABACUS	Azure	File server storing and managing shared files within the organization.
SEA-SUPPORT-01	Azure	A server used for testing the latest Windows updates before they are deployed to production servers, ensuring compatibility and stability.

The Fraxion application infrastructure is located at Azure data centers. SSO acts as a hosting subservice organization for the company. The subservice organization provides physical security and environmental protection controls, as well as managed services for Fraxion's infrastructure.

SSO's network security uses hardware and software-based intrusion prevention, advanced content filtering, anti-malware, and anti-spam modules.

In addition to the firewall, Fraxion uses anti-virus and anti-spyware applications to protect systems from viruses.

Fraxion's Information Security Policy and security procedures ensure that all computer devices (including servers, desktops, printers, etc.) connected to the Fraxion network have proper virus protection software, current virus definition libraries, and the most recent operating system and security patches installed. The IT department verifies that all known and reasonable defenses are in place to reduce network vulnerabilities while keeping the network operating. In the event of a virus threat, the anti-virus system will attempt to delete or quarantine the infected file. If the virus cannot be deleted or quarantined, the infected machine will be disconnected from the network and cleaned manually.

Multiple controls are installed to monitor traffic that could contain malicious programs or code. External perimeter scans are performed annually by a third-party vendor to expose potential vulnerabilities to the production environment and corporate data. Email is scanned at the gateway and in the hosted email environment. Server operating systems utilize anti-virus and anti-spyware programs. All employee workstation computers have a minimum standard hardware and software configuration. Employees are not allowed to install any software on Fraxion-owned computers. IT staff maintain several replacement computers that can replace workstations in need of repair or maintenance, thereby disrupting the employee's workday as little as possible.

SOFTWARE

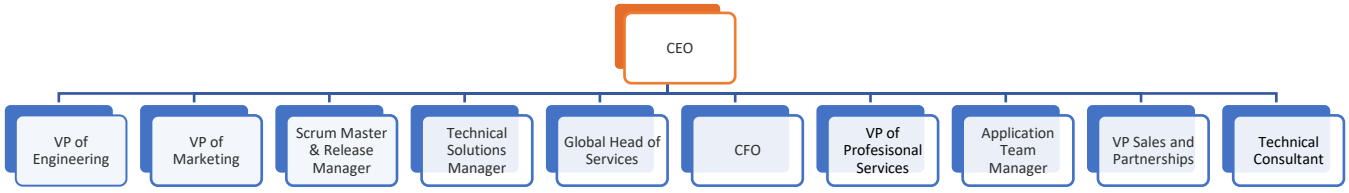
Fraxion maintains a list of critical software in use within its environment. The organization also retains appropriate software license documentation. The in-scope Fraxion software components are shown in the table provided below:

Primary Software		
System/Application	**Operating System**	**Purpose**
DevOps	Azure	Change management and CI/CD pipelines.
VPN Client	Azure	Secure connections to domain controllers and servers.
Defender for Endpoint	Microsoft	Endpoint security and threat protection.
Intune	Microsoft	Patch management and device policy enforcement. Manages and tracks devices within the organization, ensuring compliance with internal policies. Devices are enrolled for management and can be remotely monitored, updated, and secured.
HubSpot	HubSpot	Customer relation-ship management (CRM).
M365 Tools	Microsoft	Email services, including quarantine monitoring.
M365 Apps	Microsoft	Productivity suite for document editing, spreadsheets, and presentations.
Visual Studio	Microsoft	Integrated development environment (IDE) for software development.
Logic Apps	Azure	Workflow automation and integration service.
SQL Database	Azure	Managed cloud database service.

Primary Software		
System/Application	**Operating System**	**Purpose**
SQL Server Management Studio	Microsoft	Tool for managing and querying SQL Server instances.
Teams	Microsoft	Collaboration

PEOPLE

The Fraxion staff provides support for the above services. Fraxion employs dedicated team members to handle all major product functions, including operations, and support. The IT Team monitors the environment, as well as manages data backups and recovery. The Company focuses on hiring the right people for the right job as well as training them both in their specific tasks and on the ways to keep the Fraxion and its data secure. Fraxion's corporate structure includes the following roles:



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

- *Chief Executive Officer (CEO)* – Responsible for overall business strategy, decision-making, and operations. The CEO sets company goals, leads the senior leadership team, and ensures the organization's growth, profitability, and long-term success.
- *VP of Engineering* – Leads the engineering team, oversees product development, ensures technical excellence, and aligns engineering goals with business objectives. Drives innovation, manages resources, and fosters a high-performance engineering culture.
- *VP of Marketing* – Responsible for the outward communication of company initiatives. Primary role responsible for exposing new programs to prospects and existing customers and furthering the public reach of Fraxion.
- *Scrum Master & Release Manager* – Plans and coordinates smooth, timely software releases by ensuring alignment between development and deployment schedules. Removes bottlenecks and facilitates communication among teams to ensure successful releases. Facilitates Agile practices, supports team productivity, and removes obstacles to ensure successful project delivery.

- *Technical Solutions Manager* – Oversees the design, implementation, and support of technical solutions for clients. Works closely with sales, engineering, and product teams to meet technical requirements, troubleshoot issues, and ensure solutions align with customer needs and business goals.
- *Global Head of Services* – Leads and manages the delivery of services across all regions, ensuring consistency, quality, and alignment with company objectives. Oversee service operations, drives customer satisfaction, and develops strategies for service growth and innovation on a global scale.
- *CFO* – Responsible for oversight over third-party risk management process. Responsible for reviewing vendor service contracts.
- *VP of Professional Services* – Oversees the delivery of customer-facing services, such as implementation, training, and consulting. Ensures customer satisfaction, optimizes service delivery processes, and aligns service strategies with business goals to drive growth and long-term client success.
- *Application Team Manager* – Manages a team responsible for developing, implementing, and maintaining software applications. Ensures the team meets project deadlines, delivers quality solutions, and resolves technical issues while aligning with business goals and user needs.
- *VP Sales and Partnerships* – Leads sales strategy, team management, and revenue generation while cultivating and managing strategic partnerships. Driving business growth by developing relationships, expanding market presence, and ensuring alignment between sales and partnership goals.
- *Technical Consultant* – Advises on technology solutions, implements, and optimizes systems to align with business goals, and mentors' teams to ensure high-quality solutions and effective collaboration.

Sales and Marketing – This role is responsible for customer relations and working closely with both the Marketing Director and the Sales to ensure there is transparency between marketing and sales efforts.

Sales – Primary role for outbound reach to prospects and completing sales. They are also responsible for the maintenance and renewals of existing customer contracts.

Chief Technology Officer – Responsible for the technological direction and advancements of the organization. Directs the operations, engineering, and support teams to efficiently create/present new services, maintain existing ones, and help support the Fraxion customer based using the service.

Technology and Engineering – This role is responsible for the operations of the day-to-day items to maintain the integrity of the environment. This role is also responsible for the provisioning and research and development of new and upcoming services within the company.

Operations and Support – This role includes the support team and crosses over to the engineering team. It is primarily responsible for daily support aspects of the business. This

includes but is not limited to the support of end-users with day-to-day issues, as well as assist in the onboarding, implementation, and migrations of new and existing customers as part of their ongoing maintenance.

DATA

Data is categorized in the following (4) major types of data used by Fraxion:

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

Customer data is managed, processed, and stored in accordance with the relevant data protection and other regulations, with specific requirements formally established in customer agreements. Customer data is captured which is utilized by Fraxion in delivering its Spend Management Services.

Information takes many forms. It may be stored on computers, transmitted across networks, printed, or written on paper, and spoken in conversations. All employees and contractors of Fraxion are obligated to respect and, in all cases, to protect confidential and private data. Customer information, employment-related records, and other intellectual property-related records are subject to limited exceptions, confidential as a matter of law. Many other categories of records, including company and other personnel records, and records relating to Fraxion's business and finances are, as a matter of Fraxion policy, treated as confidential. Responsibility for guaranteeing appropriate security for data, systems, and networks is shared by the Client Services and IT Departments. IT is responsible for designing, implementing, and maintaining security protection and retains responsibility for ensuring compliance with the policy. In addition

to management and the technology staff, individual users are responsible for the equipment and resources under his or her control.

Fraxion has policies and procedures in place to ensure prior retention and disposal of confidential and private data. The retention and data destruction policies define the retention periods and proper destruction procedures for the disposal of data. These policies are reviewed at least annually. The destruction of data is a multi-step process. Client data is deleted upon termination of the contract. A ticket is created and assigned to the product team and system engineering team to coordinate the deletion of the data. First, all files received or generated from the client are identified and deleted by the system engineering team then the product team deletes all user-related data.

Electronic communications are treated with the same level of confidentiality and security as physical documents. Networks are protected by enterprise-class firewalls and appropriate enterprise-class virus protection is in place. Passwords protection with assigned user rights is required for access to the network, application, and databases. Access to the network, application, and databases is restricted to authorized internal and external users of the system to prohibit unauthorized access to confidential data. Additionally, access to data is restricted to authorized applications to prevent unauthorized access outside the boundaries of the system.

PROCEDURES

Formal IT policies and procedures exist that describe logical access, computer operations, change management, incident management, and data communication standards in order to obtain the stated objectives for network and data security, data privacy, and integrity for both the company and its clients and define how services should be delivered. These are communicated to employees and located within the organization’s intranet.

Reviews and changes to these policies and procedures are performed annually and are approved by senior management.

Physical Security

Fraxion’s production servers are maintained by Azure and the physical security and environmental protections are the responsibility of Azure. Management obtains and reviews SOC report annually.

Logical Access

SSO handles the network, physical host, and virtual server infrastructure. Fraxion handles the administrative responsibilities involved in supporting the web, application, database components of the platform Fraxion has full access to log into their servers remotely using secure shell (SSH) or Windows Remote Desktop, depending on the platform. Dedicated firewalls are used to restrict administrative access to servers. Appropriate firewall rules are in place to restrict access to

customer data and to limit the possibility of disruptions to customer operations from unauthorized users.

Logical access to Fraxion's networks, applications, and data is limited to properly authorized individuals. For both the client-hosted network and the Fraxion local network, logical access is controlled via standard user authentication credentials (user ID and password). No other outside access is permitted.

Backups

Fraxion maintains real-time, full system replication of the production platform between the West Europe (Primary) datacenter and the North Europe (Failover) datacenter using Azure Failover Groups. In addition, Fraxion servers utilize Azure Backup for point-in-time full and incremental backups. The retention period for these backups is 35 days, with a rotation period of daily incremental backups and weekly long-term retention (LTR) backups for 4 weeks, as well as monthly LTR backups for 12 weeks. Emails are generated on job completion, and reviews are completed daily with additional monitoring via Azure Monitor and Microsoft Defender for Cloud service alerts. Weekly backup summary emails are also generated. All backups are encrypted and stored onsite in the dedicated backup servers.

Computer Operations

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

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

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

Change Management

For internally developed software solutions, Fraxion uses an agile-based SDLC process, which includes research and planning, analysis and design, initial development, and quality assurance (QA) testing before the final release. All software development activities follow the internal project-related business process model.

A ticketing system is utilized to document the change control procedures for changes in the application and implementation of new changes. Quality assurance testing is documented and maintained with the associated change request. Development and testing are performed in an environment that is logically separated from the production environment.

Patch Management

Fraxion takes a proactive approach to patch management. The CTO and engineers regularly monitor websites, message boards, and mailing lists where advanced notifications of bug-related patches are often disclosed prior to a public announcement by the vendor. This allows the company to plan for upcoming patches.

The networking team reviews the availability of patches and independently determines if it is necessary to deploy within the production environment. Approved patches are scheduled for installation in the test environment weekly as applicable. If there are no issues in the test environment after a week, the patch will be applied to the production environment. The patching process is tracked via Azure DevOps ticket.

Problem Management

Fraxion maintains an Incident Response Policy that describes the process for identifying and addressing potential security incidents. The policy details exactly what must occur if an incident is suspected and covers both electronic and physical security incidents. Plans for detecting, responding to, and recovering from incidents are included in the policy, and post-incident activity requirements are defined. To ensure responsible employees are prepared to respond to incidents, the organization provides formal security breach training.

The organization provides a customer service request form where clients can report potential security breaches, and clients are also provided with an email and phone number for this same purpose. Internal users are directed to report incidents through an internal portal for documentation and tracking purposes.

System Monitoring

The Operations Security Policy describes the organization’s policies and procedures related to network logging and monitoring as well as vulnerability identification and remediation. The organization uses Azure for system logging within the Azure environment. Azure logs document source IP, destination IP, destination port, protocol type, and timestamp. The organization monitors system capacity using Azure Monitor Metrics.

Microsoft Defender for Cloud is used for threat detection, security posture management, and compliance monitoring. The tool continuously assesses cloud resources, identifying misconfigurations and security risks while providing recommendations for remediation. It generates logs, VPC flow logs, and DNS logs, contributing to intrusion detection and attack surface reduction. Defender for Cloud monitors and protects workloads across virtual machines, storage, and databases, ensuring security configurations align with industry standards. The solution leverages behavioral analytics and AI-driven detections to identify advanced threats, helping the organization proactively mitigate risks.

The vulnerability assessment process involves the execution of CIS testing, implementation of antivirus software, and system patching. The organization uses Microsoft Defender for Endpoint antivirus and has configured the software to run updates daily and prohibit end-users from disabling or altering the software. Alerts are sent immediately when a potential virus is detected, and logs are generated and retained for at least one year, with at least three months readily available. Azure Security Center is used to identify newly emerging vulnerabilities, and the organization monitors vendors for patch updates to correct vulnerabilities.

Vendor Management

The organization maintains an Operations Security Policy that includes requirements for interacting with vendors/service providers. The policy includes requirements for performing due diligence measures prior to engaging with a new provider. Due diligence procedures include evaluating each material IT vendors' cost-effectiveness, functionality/services, risk, financial viability, compliance, and performance. The organization is required to define service levels when negotiating an arrangement with a new vendor or re-negotiating an existing arrangement, and all service levels are agreed upon and documented clearly. The organization monitors its providers' service levels to ensure each provider is providing the agreed-upon services and is compliant with all requirements. The organization executes non-disclosure agreements with third parties before any information is shared.

Data Communications

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

The PaaS provider also automates the provisioning and deprovisioning of containers to match the desired configuration; if an application container fails, it will be automatically replaced, regardless of whether that failure is in the application or on underlying hardware.

Boundaries of the System

The boundaries of Fraxion's Spend Management Services System are the specific aspects of the Company's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of the Fraxion's Spend Management Services System.

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

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

The Security category, and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. Security, and the controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security criteria are included in Section 4 of this report. Although the applicable trust services criteria and related controls are included in Section 4, they are an integral part of the Fraxion's description of its system.

CONTROL ENVIRONMENT

The control environment is the set of standards, processes, and structures that provide the basis for carrying out internal control across an organization. The organizational structure, separation of job responsibilities by departments and business function, documentation of policies and procedures, and internal audits are the methods used to define, implement and assure effective operational controls. The Board of Directors and/or senior management establish the tone at the top regarding the importance of internal control and expected standards of conduct.

Integrity and Ethical Values

Fraxion's control environment reflects the philosophy of senior management concerning the importance of the security of data. Integrity and ethical values are essential elements of Fraxion's control environment. Management is responsible for setting the tone at the top, establishing, communicating, and monitoring control policies and procedures.

Formal policies, code of employment practice, and Code of Conducts are documented and communicated to employees to ensure that entity values, ethics, integrity, and behavioral standards are a primary focus, and risks are mitigated in daily operations. In addition, a sanctions policy is in place to address deviations from established security and personnel standards.

Management's philosophy and operating style affect the way the entity is managed, including the kinds of business risks accepted. Fraxion places a great deal of importance on working to ensure that the integrity of processing is a primary focus and that controls are maximized to mitigate risk in daily operations. Management and specific teams are structured to ensure the highest level of integrity and efficiency in customer support and transaction processing.

Formal job descriptions and departmental meetings and staff interactions ensure communication of organizational values, ethics, and behavior standards. Personnel operates under Fraxion's policies and procedures, including confidentiality agreements and security policies. Annual training is conducted to communicate regulations and the importance of privacy and security.

Management is committed to being aware of regulatory and economic changes that impact lines of business and monitoring the customer base for trends, changes, and anomalies.

Commitment to Competence

Fraxion has standardized human resource policies and procedures. The result is a uniform set of practices that provide equitable hiring and advancement opportunities across the organization. Training and development opportunities are provided to staff and performance evaluations are performed to communicate goals based on job responsibilities and address any performance issues.

Employees are trained in their specific roles and policies through on-the-job training and procedures are reviewed. Management communicates any changes to these policies on an ongoing basis and policies are updated as needed. In order to protect confidential internal and client information employees are prohibited from divulging any information regarding client affairs or taking action, not in the interests of the client or Fraxion.

Management's Philosophy and Operating Style

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

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

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

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

Organizational Structure and Assignment of Authority and Responsibility

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

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

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

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

Human Resources Policies and Procedures

Fraxion has formal hiring procedures that are designed to ensure that new team members are able to meet or exceed the job requirements and responsibilities. All candidates go through interviews and assessments of their education, professional experience, and certifications. Background checks are performed for all newly hired employees before the start date and include a review of their education and criminal records.

During the onboarding process, the new employees review the Code of Conduct, code of employment practice, and any other relevant policies and procedures relevant to their role. Newly hired employees are required to sign an acknowledgment of receipt and understanding of the Code of Conduct and code of employment practice. These policies and procedures are also available to employees through the internal policies repository. Security awareness training is also completed at least annually by all employees. That includes the areas of security and confidentiality to communicate the security implications around their roles and how their actions could affect the organization.

Ongoing performance feedback is provided to all employees and contractors. Formal performance reviews are completed annually by management to discuss expectations, goals, and the employees' performance for the last fiscal year.

RISK ASSESSMENT PROCESS

Fraxion regularly reviews the risks that may threaten the achievement of its service commitments and system requirements related to security. The Risk assessment process is performed by management to identify and manage risks and consider possible changes in the internal and external environment to mitigate these risks. Risk mitigation activities include the prevention, mitigation, and detection of risk via the implementation of internal controls. In addition, management also transfers risk through the organization's business insurance policies.

The Fraxion management team and other members of the engineering team monitor rick on an ongoing basis using information derived from employee input, monitoring system audit results, industry experience, business environment, and internal system and/or process changes.

On an annual basis, management completes a risk assessment as part of the annual risk management activities. Risks identified during the annual risk assessment process include the following:

- Operational Risk
- Strategic Risk
- Compliance Risk
- Fraud Risk
- Environmental Risk

Integration with Risk Assessment

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

INFORMATION AND COMMUNICATION SYSTEM

Fraxion has an information security policy to help ensure that employees understand their roles and responsibilities concerning processing and controls to ensure significant events are communicated in a timely manner. These include formal and informal training programs and the use of email to communicate time-sensitive information and processes for security, confidentiality, and availability purposes that notify the key personnel in the event of problems.

Additional communication methods include department meetings to communicate company policies, procedures, industry or business issues, or other topics management deems key to the achievement of the organization's objectives. Communication is encouraged at all levels to promote the operating efficiency of Fraxion.

Fraxion also updates their website on an ongoing basis to inform clients and other external parties of company and industry-related issues that could affect their services and what steps the company is taking to reduce or avoid the impact on their operations. The organization's security commitments regarding the Spend Management services system are included in the services agreement.

MONITORING CONTROLS

In addition to daily oversight and vulnerability assessments, management uses monitoring software to monitor the security and availability of their systems. Ongoing monitoring of internal controls is also performed by management.

Ongoing Monitoring

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

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

Monitoring of the Subservice Organization

Fraxion uses a subservice organization to provide hosting services.

Management of Fraxion receives and reviews the SOC 2 report of Azure on an annual basis. In addition, through its daily operational activities, the management of Fraxion monitors the services performed by Azure to ensure that operations and controls expected to be implemented at the subservice organization are functioning effectively.

Reporting Deficiencies

Fraxion's internal risk management tracking tool is utilized to document and track the results of on-going monitoring procedures. Escalation procedures are maintained for responding and notifying management of any identified risks, and instructions for escalation are supplied to employees in company policy documents. Risks receiving a high rating are responded to immediately. Corrective actions, if necessary, are documented and tracked within the internal tracking tool. Annual risk meetings are held for management to review reported deficiencies and corrective actions.

CHANGES TO THE SYSTEM AFTER THE EXAM DATE

No significant changes have occurred to the services provided to user entities since the exam date.

SYSTEM INCIDENTS AFTER THE EXAM DATE

No significant incidents have occurred to the services provided to user entities since the exam date.

COMPLEMENTARY SUBSERVICE ORGANIZATION CONTROLS (CSOCs)

Fraxion's controls related to the System cover only a portion of overall internal control for each user entity of Fraxion. It is not feasible for the trust services criteria related to the System to be achieved solely by Fraxion. Therefore, each user entity's internal controls should be evaluated in conjunction with Fraxion's controls and the related tests and results described in Section 4 of this report, taking into account the related complementary subservice organization controls expected to be implemented at the subservice organization as described below.

#	Complementary Subservice Organization Controls (CSOC)	Related Criteria
1	Azure is responsible for maintaining physical security and environmental protection controls over the data centers hosting the Fraxion infrastructure.	CC6.4
2	Azure is responsible for the destruction of physical assets hosting the production environment.	CC6.5

COMPLEMENTARY USER ENTITY CONTROLS (CUECs)

Fraxion's controls related to the Fraxion's Spend Management Services system only cover a portion of the overall internal controls for each user entity. It is not feasible for the applicable trust services criteria related to the system to be achieved solely by Fraxion control procedures. Accordingly, user entities, in conjunction with the services, should establish their internal controls or procedures to complement those of Fraxion.

User auditors should determine whether the following controls have been in place in operation at the user organization:

1. User entities should have controls in place to provide reasonable assurance that user access including the provisioning and de-provisioning are designed appropriately and operating effectively.
2. User entities are responsible for reporting issues with Fraxion systems and platforms.
3. User entities are responsible for understanding and complying with their contractual obligations to Fraxion.
4. User entities are responsible for notifying Fraxion of changes made to the administrative contact information.

TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

The Security category and applicable trust services criteria were used to evaluate the suitability of the design of controls stated in the description. The criteria and controls designed, implemented, and operated to meet them ensure that information, systems, and access (physical and logical) are protected against unauthorized access, and systems are available for operation and use. The controls supporting the applicable trust services criteria are included in Section 4 of this report and are an integral part of the description of the system.

For specific criteria, which were deemed not relevant to the system, see Section 4 for the related explanation.

SECTION 4: TRUST SERVICES CATEGORY, CRITERIA, AND RELATED CONTROLS

Trust Services Category, Criteria, and Related Controls

This SOC 2 Type 1 report was prepared in accordance with the AICPA attestation standards and has been performed to examine the suitability of the design of controls to meet the criteria for the Security category set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (With Revised Points of Focus—2022)* in AICPA*, Trust Services Criteria* as of November 1, 2024.

The applicable trust services criteria and related controls specified by Fraxion are presented in Section 4 of this report.

On the pages that follow, the applicable trust services criteria and the control activities to achieve the applicable trust services criteria have been specified by and are the responsibility of Fraxion.

CONTROL ACTIVITIES SPECIFIED BY THE SERVICE ORGANIZATION

CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	**Client Controls**
Criteria: COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.	
CC1.1.1	The company has an approved Code of Conduct that is reviewed annually and updated as needed.
CC1.1.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.
CC1.1.3	The company requires employees and contractors to review and acknowledge the information security policies at the time of hire and active employees and contractors to acknowledge the information technology security policies at least annually.
CC1.1.4	The company performs background checks on new employees.
CC1.1.5	The company's employees sign a confidentiality agreement during onboarding.
CC1.1.6	The company managers perform a complete performance evaluation for direct reports at least annually.
Criteria: COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.	
CC1.2.1	The company's board members have sufficient expertise to oversee management's ability to design, implement and operate information security controls.
CC1.2.2	The company's board of directors meets at least annually and maintains formal meeting minutes.
CC1.2.3	The company has an InfoSec Roles Policy that outlines the board of directors' responsibilities for oversight of internal controls.
CC1.2.4	The company's board of directors consists of members that are independent from the company.
Criteria: COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.	
CC1.3.1	The company has an InfoSec Roles Policy that outlines the board of directors' responsibilities for oversight of internal controls.
CC1.3.2	The company maintains an organizational chart that describes the organizational structure and reporting lines.
CC1.3.3	The company requires employees and contractors to review and acknowledge the information security policies at the time of hire and active employees and contractors to acknowledge the information technology security policies at least annually.
CC1.3.4	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the InfoSec Roles Policy.

CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ENVIRONMENT	
Control Number	**Client Controls**
Criteria: COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.	
CC1.4.1	The company performs background checks on new employees.
CC1.4.2	The company managers complete a performance evaluation for direct reports at least annually.
CC1.4.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the InfoSec Roles Policy.
CC1.4.4	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees to complete security training at least annually.
Criteria: COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.	
CC1.5.1	The company managers perform complete a performance evaluation for direct reports at least annually.
CC1.5.2	The company requires employees and contractors to acknowledge the Code of Conduct at the time of hire and active employees and contractors to acknowledge the Code of Conduct at least annually.
CC1.5.3	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the InfoSec Roles Policy.

CRITERIA FOR THE SECURITY CATEGORY INFORMATION AND COMMUNICATION	
Control Number	**Client Controls**
Criteria: COSO Principle 13: The entity obtains or generates and uses relevant quality information to support the functioning of internal control.	
CC2.1.1	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC2.1.3	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
CC2.1.4	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.
CC2.1.5	Vulnerability scans are required to be performed continuously on all external-facing systems. Critical and high vulnerabilities are required to be tracked to remediation.
Criteria: COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.	
CC2.2.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC2.2.2	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the InfoSec Roles Policy.
CC2.2.3	The company requires new employees and contractors to complete security awareness training at the time of hire and active employees to complete security training at least annually.
CC2.2.4	The company's information security policies and procedures are documented and reviewed at least annually.
CC2.2.5	The company provides a description of its products and services to internal and external users.
CC2.2.6	The company communicates system changes to authorized internal users.
Criteria: COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.	
CC2.3.1	The company's security commitments are communicated to customers in the Privacy Policy and Terms of Service (TOS).
CC2.3.2	The company provides a description of its products and services to internal and external users.
CC2.3.3	The company notifies customers of critical system changes that may affect their processing.
CC2.3.4	The company provides guidelines and technical support resources relating to system operations to customers.
CC2.3.5	Contact information for users to report system information on failures, incidents, concerns, and other complaints to appropriate personnel is available.

CRITERIA FOR THE SECURITY CATEGORY INFORMATION AND COMMUNICATION	
Control Number	**Client Controls**
CC2.3.6	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality commitments applicable to that entity.

CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Client Controls**
Criteria: COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.	
CC3.1.1	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC3.1.2	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
Criteria: COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.	
CC3.2.1	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC3.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security and privacy requirements; and - annual review of critical vendors.
CC3.2.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.2.4	The company has a documented disaster recovery (DR) plan and requires that it be tested quarterly.
Criteria: COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.	
CC3.3.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.3.2	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

CRITERIA FOR THE SECURITY CATEGORY	
RISK ASSESSMENT	
Control Number	**Client Controls**
Criteria: COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.	
CC3.4.1	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
CC3.4.2	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.
CC3.4.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC3.4.4	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.

CRITERIA FOR THE SECURITY CATEGORY	
MONITORING ACTIVITIES	
Control Number	**Client Controls**
Criteria: COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.	
CC4.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC4.1.2	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.
CC4.1.3	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security and privacy requirements; and - annual review of critical vendors.
CC4.1.4	Vulnerability scans are required to be performed continuously on all external-facing systems. Critical and high vulnerabilities are required to be tracked to remediation.
Criteria: COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.	
CC4.2.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC4.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security and privacy requirements; and - annual review of critical vendors.
CC4.2.3	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.

CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Client Controls**
Criteria: COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.	
CC5.1.1	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.1.2	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.1.3	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC5.1.4	Role-based access is configured within Azure to enforce segregation of duties and restrict access to confidential information.
Criteria: COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.	
CC5.2.1	The company's Information Technology Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC5.2.2	The company has an Operations Security Policy and a Software Development Policy in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.2.3	The company's information security policies and procedures are documented and reviewed at least annually.
Criteria: COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.	
CC5.3.1	The company's information security policies and procedures are documented and reviewed at least annually.
CC5.3.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
CC5.3.3	The company has an Operations Security Policy and a Software Development Policy in place that governs the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC5.3.4	The company has security incident response policies and procedures that are documented and communicated to authorized users.

CRITERIA FOR THE SECURITY CATEGORY	
CONTROL ACTIVITIES	
Control Number	**Client Controls**
CC5.3.5	The company specifies its objectives to enable the identification and assessment of risk related to the objectives.
CC5.3.6	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
CC5.3.7	Roles and responsibilities for the design, development, implementation, operation, maintenance, and monitoring of information security controls are formally assigned in the InfoSec Roles Policy.
CC5.3.8	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security and privacy requirements; and - annual review of critical vendors.
CC5.3.9	The company's Information Technology Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC5.3.10	The company's Incident Response Plan documents requirements for backup and recovery of customer data.
CC5.3.11	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.

CRITERIA FOR THE SECURITY CATEGORY LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Client Controls**
Criteria: CC6.1: The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.	
CC6.1.1	The company's Information Technology Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.1.2	The company has an Information Technology Security Policy in place to help ensure that confidential data is properly secured and restricted to authorized personnel.
CC6.1.3	The company's datastores housing sensitive customer data are encrypted at rest.
CC6.1.4	The company requires that privileged access to encryption keys be restricted to authorized users with a business need.
CC6.1.5	Role-based access is configured within Azure to enforce segregation of duties and restrict access to confidential information.
CC6.1.6	The company restricts that privileged access to applications, databases, and supporting cloud infrastructure be restricted to authorized users with a business need.
CC6.1.7	Firewalls are configured to prevent unauthorized access.
CC6.1.8	The company requires that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
CC6.1.9	The company passwords for in-scope system components are configured according to the company's policy.
CC6.1.10	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
CC6.1.11	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.1.12	The company maintains a formal inventory of production system assets.
CC6.1.13	The company requires authentication to the "production network" to use unique usernames and passwords.
Criteria: CC6.2: Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.	
CC6.2.1	The company's Information Technology Security Policy documents the requirements for the following access control functions: - adding new users;

CRITERIA FOR THE SECURITY CATEGORY LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Client Controls**
	- modifying users; and/or - removing an existing user's access.
CC6.2.2	The company conducts periodic access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.2.3	Logical access to systems is revoked as a component of the termination process within the Company's SLAs.
CC6.2.4	The company requires that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
CC6.2.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.2.6	The company requires authentication to the "production network" to use unique usernames and passwords.
Criteria: CC6.3: The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.	
CC6.3.1	The company's Information Technology Security Policy documents the requirements for the following access control functions: - adding new users; - modifying users; and/or - removing an existing user's access.
CC6.3.2	The company conducts periodic access reviews for the in-scope system components to help ensure that access is restricted appropriately. Required changes are tracked to completion.
CC6.3.3	Logical access to systems is revoked as a component of the termination process within the Company's SLAs.
CC6.3.4	The company requires that user access to in-scope system components is based on job role and function or requires a documented access request form and manager approval prior to access being provisioned.
CC6.3.5	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.3.6	The company requires authentication to the "production network" to use unique usernames and passwords.
Criteria: CC6.4: The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.	
CC6.4.1	Management contracts with Azure to provide physical and logical access security of its production systems; therefore, this criterion is carved out.

CRITERIA FOR THE SECURITY CATEGORY LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Client Controls**
Criteria: CC6.5: The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.	
CC6.5.1	The company has formal retention and disposal procedures in place to guide the secure retention and disposal of company and customer data.
CC6.5.2	The company has electronic media containing confidential information purged or destroyed in accordance with best practices, and certificates of destruction are issued for each device destroyed.
CC6.5.3	Logical access to systems is revoked as a component of the termination process within the Company's SLAs.
CC6.5.4	The destruction of physical assets hosting the production environment is the responsibility of Azure. Refer to the subservice organization's section above for controls managed by the subservice organization.
Criteria: CC6.6: The entity implements logical access security measures to protect against threats from sources outside its system boundaries.	
CC6.6.1	The company's production systems can only be remotely accessed by authorized employees via an approved encrypted connection.
CC6.6.2	The company's production systems can only be remotely accessed by authorized employees possessing a valid multi-factor authentication (MFA) method.
CC6.6.3	Firewalls are configured to prevent unauthorized access.
CC6.6.4	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.
CC6.6.5	The company requires a compliance tool to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC6.6.6	The company has infrastructure supporting the service patched or updated as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC6.6.7	The company's network and system hardening standards are required and documented, based on industry best practices, and reviewed at least annually.
CC6.6.8	The company requires authentication to the "production network" to use unique usernames and passwords.
Criteria: CC6.7: The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.	
CC6.7.1	The company encrypts workstations to protect sensitive data.
CC6.7.2	The company uses secure data transmission protocols to encrypt confidential and sensitive data when transmitted over public networks.

CRITERIA FOR THE SECURITY CATEGORY LOGICAL AND PHYSICAL ACCESS CONTROLS	
Control Number	**Client Controls**
CC6.7.3	The company has a mobile device monitoring system (MDM) in place to centrally monitor mobile devices supporting the service.
Criteria: CC6.8: The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.	
CC6.8.1	The company deploys anti-malware technology to environments commonly susceptible to malicious attacks and configures this to be updated routinely, logged, and installed on all relevant systems.
CC6.8.2	The company has an Operations Security Policy and a Software Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC6.8.3	The company has infrastructure supporting the service patched or updated as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.

CRITERIA FOR THE SECURITY CATEGORY SYSTEM OPERATIONS	
Control Number	**Client Controls**
Criteria: 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.	
CC7.1.1	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
CC7.1.2	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC7.1.3	The company has a configuration management procedure in place to ensure that system configurations are deployed consistently throughout the environment.
CC7.1.4	The company's formal policies outline the requirements for the following functions related to the IT and Security Analysts: - vulnerability management; - system monitoring.
Criteria: CC7.2: The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.	
CC7.2.1	The company uses a compliance tool to provide continuous monitoring of the company's network and early detection of potential security breaches.
CC7.2.2	The company utilizes a log management tool to identify events that may have a potential impact on the company's ability to achieve its security objectives.
CC7.2.3	The company's formal policies outline the requirements for the following functions related to the IT and Security Analysts: - vulnerability management; - system monitoring.
CC7.2.4	The company has infrastructure supporting the service patched or updated as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC7.2.5	An infrastructure monitoring tool is required to be utilized to monitor systems, infrastructure, and performance and generates alerts when specific predefined thresholds are met.
CC7.2.6	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.

CRITERIA FOR THE SECURITY CATEGORY SYSTEM OPERATIONS	
Control Number	**Client Controls**
CC7.2.7	Security incidents are reported to the IT personnel and tracked through to resolution in a ticketing system.
CC7.2.8	Vulnerability scans are required to be performed continuously on all external-facing systems. Critical and high vulnerabilities are required to be tracked to remediation.
Criteria: CC7.3: The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.	
CC7.3.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC7.3.2	The company's security and privacy incidents are required to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
Criteria: CC7.4: The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.	
CC7.4.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC7.4.2	The company's security and privacy incidents are required to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.4.3	The company has infrastructure supporting the service patched or updated as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC7.4.4	Vulnerability scans are required to be performed continuously on all external-facing systems. Critical and high vulnerabilities are required to be tracked to remediation.
CC7.4.5	The company requires to test their incident response plan at least annually.
Criteria: CC7.5: The entity identifies, develops, and implements activities to recover from identified security incidents.	
CC7.5.1	The company has security incident response policies and procedures that are documented and communicated to authorized users.
CC7.5.2	The company's security and privacy incidents are required to be logged, tracked, resolved, and communicated to affected or relevant parties by management according to the company's security incident response policy and procedures.
CC7.5.3	The company requires to test their incident response plan at least annually.
CC7.5.4	The company has a documented disaster recovery (DR) plan and requires that it be tested quarterly.

CRITERIA FOR THE SECURITY CATEGORY	
CHANGE MANAGEMENT	
Control Number	**Client Controls**
Criteria: CC8.1: The entity authorizes, designs, develops, or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.	
CC8.1.1	The company has an Operations Security Policy and a Software Development Policy in place that govern the development, acquisition, implementation, changes (including emergency changes), and maintenance of information systems and related technology requirements.
CC8.1.2	The company requires changes to software and infrastructure components of the service to be authorized, formally documented, tested, reviewed, and approved prior to being implemented in the production environment.
CC8.1.3	The company restricts access to migrate changes to production to authorized personnel.
CC8.1.4	The company's penetration testing is required to be performed annually. A remediation plan is required to be developed, and changes are required to be implemented to remediate vulnerabilities in accordance with SLAs.
CC8.1.5	The company has infrastructure supporting the service patched or updated as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC8.1.6	The company's network and system hardening standards are required and documented, based on industry best practices, and reviewed at least annually
CC8.1.7	Vulnerability scans are required to be performed continuously on all external-facing systems. Critical and high vulnerabilities are required to be tracked to remediation.
CC8.1.8	The company’s risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.

CRITERIA FOR THE SECURITY CATEGORY	
RISK MITIGATION	
Control Number	**Client Controls**
Criteria: CC9.1: The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.	
CC9.1.1	The company's risk assessments are performed at least annually. As part of this process, threats, and changes (environmental, regulatory, and technological) to service commitments are identified and the risks are formally assessed. The risk assessment includes a consideration of the potential for fraud and how fraud may impact the achievement of objectives.
CC9.1.2	The company has a documented risk management program that includes guidance on the identification of potential threats, rating the significance of the risks associated with the identified threats, and mitigation strategies for those risks.
Criteria: CC9.2: The entity assesses and manages risks associated with vendors and business partners.	
CC9.2.1	The company has written agreements in place with vendors and related third parties. These agreements include confidentiality commitments applicable to that entity.
CC9.2.2	The company has a vendor management program in place. Components of this program include: - critical vendor inventory. - vendor's security and privacy requirements; and - annual review of critical vendors.