Service Organization Control 2 (SOC 2®) Type 2 Report

Report on VersaFile's description of its Technical and Managed Services and on the suitability of the design and operating effectiveness of controls relevant to Security for the period April 1, 2023 to September 30, 2023

This report is intended solely for use by the management of VersaFile and the specified parties, and is not intended and should not be used by anyone other than these parties.

Table of Contents

Section I

VersaFile's Management Assertion

VersaFile's Management Assertion

We have prepared the attached description titled "VersaFile's Description of its Technical and Managed Services" throughout the period April 1, 2023 to September 30, 2023 ("description") based on the criteria for a description of a service organization's system in DC section 200 *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*) ("description criteria"). The description is intended to provide users with information about the VersaFile Services that may be useful when assessing the risks arising from interactions with VersaFile's ("VersaFile") Technical and Managed Services, particularly information about system controls that VersaFile has designed and implemented to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, (AICPA, *Trust Services Criteria*).

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

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

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

1. The description presents VersaFile's Technical and Managed Services that was designed and implemented throughout the period April 1, 2023 to September 30, 2023 in accordance with the description criteria.
2. The controls stated in the description were suitably designed throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that

VersaFile's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of VersaFile's controls throughout the period April 1, 2023 to September 30, 2023.

3. The controls stated in the description operated effectively throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that VersaFile's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of VersaFile's controls, operated effectively throughout the period April 1, 2023 to September 30, 2023.

DocuSigned by:
Tayo Runsewe
CF146BE525484FD...

Tayo Runsewe, CEO
VersaFile
February 21, 2024

Section II

Independent Service Auditor's Report

Independent Service Auditor's Report

To the Management of VersaFile:

Scope

We have examined VersaFile's attached description titled "VersaFile's Description of its Technical and Managed Services" throughout the period April 1, 2023 to September 30, 2023, ("description") based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2® Report* (AICPA, *Description Criteria*), ("description criteria") and the suitability of the design and operating effectiveness of controls stated in the description throughout the period April 1, 2023 to September 30, 2023, to provide reasonable assurance that VersaFile's ("VersaFile") service commitments and system requirements were achieved based on the trust services criteria relevant to Security ("applicable trust services criteria") set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

VersaFile uses subservice organizations to provide cloud infrastructure services. The description indicates that complementary subservice organization controls that are suitably designed and implemented are necessary, along with controls at VersaFile to achieve VersaFile's service commitments and system requirements based on the applicable trust services criteria. The description presents VersaFile's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of VersaFile's controls. The description does not disclose the actual controls at the subservice organizations. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and implemented are necessary, along with controls at VersaFile, to achieve VersaFile's service commitments and system requirements based on the applicable trust services criteria. The description presents VersaFile's controls, the applicable trust

services criteria, and the complementary user entity controls assumed in the design of VersaFile's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design of such controls.

Service organization's responsibilities

VersaFile is responsible for its service commitments and system requirements and for designing, implementing and operating controls within the system to provide reasonable assurance that VersaFile's service commitments and system requirements were achieved. In Section I, VersaFile has provided the accompanying assertion titled "VersaFile's Management Assertion" ("assertion"), about the description and the suitability of the design of controls stated therein. VersaFile 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.

Our independence and quality control

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

Service auditors' responsibilities

Our responsibility is to express an opinion on the description and on the suitability of the design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with the Canadian Standard on Assurance Engagements 3000, Attestation Engagements Other Than Audits or Reviews of Historical Financial Information, set out in the *CPA Canada Handbook – Assurance* and with attestation standards established by the American Institute of Certified Public Accountants (AICPA). These 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 effectively to provide reasonable assurance that the service organization's service commitments and system requirements were achieved based on the applicable trust services criteria. We believe that the evidence we obtained is sufficient and appropriate to provide a reasonable basis for our opinion.

An examination of the description of a service organization's system and the suitability of the design and operating effectiveness of controls involves the following:

- Obtaining an understanding of the system and the service organization's service commitments and system requirements
- Assessing the risks that the description is not presented in accordance with the description criteria and that controls were not suitably designed
- Performing procedures to obtain evidence about whether the description is presented in accordance with the description criteria
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Testing the operating effectiveness of controls stated in the description to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria
- Evaluating the overall presentation of the description
- 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 users may consider important to meet their informational needs.

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

Because of their nature, controls may not always operate effectively to achieve the service organization's service commitments and system requirements based on the applicable trust services criteria. Also, 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.

Description of Tests of Controls

The specific controls tested and the nature, timing and results of those tests are listed in section IV.

Opinion

In our opinion, in all material respects,

a. The description presents VersaFile's VersaFile Services that was designed and implemented throughout the period April 1, 2023 to September 30, 2023 in accordance with the description criteria.
b. The controls stated in the description were suitably designed throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that VersaFile's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout the period and if the subservice organizations and user entities applied the complementary controls assumed in the design of VersaFile's controls throughout the period April 1, 2023 to September 30, 2023.
c. The controls stated in the description operated effectively throughout the period April 1, 2023 to September 30, 2023 to provide reasonable assurance that VersaFile's service commitments and system requirements were achieved based on the applicable trust services criteria, if complementary subservice organization controls and complementary user entity controls assumed in the design of

VersaFile's controls, operated effectively throughout the period April 1, 2023 to September 30, 2023.

Restricted use

This report, is intended solely for the information and use of VersaFile; user entities of VersaFile's Technical and Managed Services throughout the period April 1, 2023 to September 30, 2023, business partners of VersaFile subject to risks arising from interactions with the Technical and Managed Services, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

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

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

DocuSigned by:
MHM Professional Corporation
4F227774372B4BC...

Chartered Professional Accountant
Calgary, Alberta
February 21, 2024

Section III

VersaFile's Description of its VersaFile Services

Purpose and Scope of Report

This report on the internal controls placed in operation is intended to provide interested parties with sufficient information to obtain an understanding of those aspects of VersaFile controls that may be relevant to a user organization's internal control structure, based on the criteria to meet the Security categories as set forth in TSP Section 100, 2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy (AICPA, Trust Services Criteria).

The purpose of this report is to provide information on the internal controls of VersaFile as they relate to the in-scope services VersaFile provides to customers.

This report is intended to assist user entities in determining the adequacy of the internal controls that are outsourced to VersaFile and are relevant to their internal control structures as it relates to Security risks.

Company Overview

VersaFile is a privately held technology company founded in 2006 and headquartered in Vancouver, British Columbia, Canada, with a subsidiary office in Seattle, Washington, USA. Industries served include a wide array of areas, including (but not limited to):

- Automotive
- Consumer Goods
- Education
- Energy and Utilities
- Financial Services
- Government
- Healthcare
- High Tech
- Life Sciences
- Manufacturing
- Media and Entertainment
- Metals and Mining
- Oil and Gas
- Real Estate
- Retail
- Travel and Transportation

Services Provided

VersaFile Technical Services deliver Technology Projects, Managed Services , and Support Services (hereafter referred to as the "VersaFile Services").

Technical Project delivery is technology agnostic and focussed on delivering projects to meet business needs around content and intelligent automation.

Managed Services include Application Managed Services, SaaS, and PaaS offerings related to Content and Intelligent Automation Technologies.

Support Services provide support for several content and intelligent automation technologies against client required SLA and support tiers.

VersaFile Services are offered as a customer-hosted option where VersaFile staff will work with the customer staff to install, deploy and configure software in the customer's environment. Additionally, VersaFile Services are available as a VersaFile-owned and managed instance on a cloud platform (hereafter referred to as the "SaaS Solution").

Principal Service Commitments and System Requirements

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

Security commitments to user entities are documented in customer agreements. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental designs of the VersaFile Services that are designed to permit system users to access the information they need based on the permission of least privilege provisioning.
- Use of encryption protocols to protect customer data at rest and in transit as applicable.

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

Subservice Organizations

VersaFile relies on services performed by the following subservice organizations in order to deliver components of the control activities and to meet its service commitments over its VersaFile Services:

Subservice Organizations	Services Provided by Subservice Organizations
Microsoft Azure	VersaFile uses Microsoft Azure to provide cloud and data hosting services for the VersaFile Services.

The list of control activities expected to be implemented at each Subservice organization is described in the Complementary Subservice Organization Controls section below.

Components of the System Used to Provide the Services

Infrastructure

In the SaaS Solution, all customers receive their own logical tenant in the cloud platform; customer data is logically separated and not accessible to other tenants to prevent unauthorized access. At a minimum, the SaaS Solutions are deployed within the respective cloud platform leveraging that platform's security reference architecture. Where a customer has a greater level of governance required, VersaFile will implement the required security architecture as per the specific customer or project, defined in the appropriate design and implementation documentation.

The specific ECM and Intelligent Automation applications that run vary depending on customer requirements.

Software

The following provides a summary of software systems used to deliver VersaFile VersaFile Services:

- **DataDog** – log processing and alerting services.
- **Keeper Security** – credential management services for access to the VersaFile Services.
- **IBM FileNet** – platform for the delivery of Enterprise Content Management.
- **GitHub** – used for source code version control.
- **Atlassian -** Jira Service Management to provide management of customer support ticketing.
- **Microsoft 365** - management of service related content and communication.
- **Microsoft Azure Active Directory** - authentication and authorization services.

People

VersaFile has a defined organizational structure with specific roles, responsibilities, and appropriate lines of reporting required to support the VersaFile Services. It is comprised of, and supported by, the following teams who are responsible for the delivery and management of the system:

- **Management** – responsible for providing the overall direction, strategic vision, and management of VersaFile.
- **Managed Services Team** – responsible for the planning, management, and operation of Managed Services and SaaS offerings.
- **Technical Services** – responsible for delivery of technical projects and engagements with clients.
- **Customer Support Team** - responsible for provision and delivery of incident management through the support desk.
- **Operations** – responsible for day-to-day operations such as document processing and office functions.
- **Sales** – responsible for development of new business related to the VersaFile services.

- **Customer Success** - responsible for successful onboarding of customers to the various services and ensuring customers derive the maximum value from their investment with VersaFile.

The teams and associated initiatives, workstreams, and functions are led by the executive management leads.

Policies, Processes & Procedures

Management has developed and communicated to employees and contractors a set of policies, processes, and procedures in several operational areas which support the Security objectives of the VersaFile Services. As part of the wider Information Security Management Program, VersaFile has developed and organized the following policies and procedure documents that are used to support the VersaFile Services.

The following policies and procedures are available to employees and contractors through the Managed Services and Technical Services:

- Acceptable Use
- Access Control
- Business Continuity and Disaster Recovery
- Change Management
- Corporate Ethics
- Customer Support and SLA
- Data Retention and Disposal
- Incident Management
- Information Security
- IT Asset Management
- Key Management and Cryptography
- Network Security
- Personnel Security
- Risk Assessment
- Server Security
- Software Development
- Vendor Management
- Vulnerability Management
- Workstation Security

Control activities have been placed into operation to help ensure that actions are carried out properly and efficiently to achieve policies and procedures compliance. VersaFile has applied a risk management approach to the organization in order to select and develop control activities. After relevant risks have been identified and evaluated, controls are established, implemented, monitored, reviewed, and improved when necessary to meet the applicable trust services criteria and the overall objective of the organization.

Data

Data in VersaFile Services is entered via the client web application, which varies from customer engagement to customer engagement. The data is processed and written to the database instance. Data transmission is secured using TLS 1.2, PKCS #1 v2.2, SHA-512 with RSA Encryption, and does not leave the VPC.

Data replication channels are also encrypted and transmitted via the private connection. All data access requests require an ACL context which contains both the authenticated user and the organization that is requesting the data. These requests are validated via the VersaFile permissions system to exclude the possibility of cross-client data leakage. All data at rest is encrypted using AES-256 encryption.

VersaFile provides a system that forms a system of record for the Information Security Management System of an enterprise. This solution collects data only from authorized users and does not collect any data from public sources, social media or the Internet. VersaFile Services may collect data from other enterprise systems but only via partner APIs and authorized users.

System Boundaries

System boundaries pertaining to the collection, use, retention, disclosure, and disposal or anonymization or personalization of data, are governed by contract provisions for particular service engagements. Data is not utilized or disclosed to third-parties outside of the scope allowed in such contracts and agreements.

Significant Changes to the System Throughout the Examination Period

There were no significant changes to the VersaFile Services throughout the examination period.

Control Environment

The control environment is determined by the control consciousness of an organization, which sets the tone of an organization and the way personnel conduct their activities, influencing how they carry out their control functions. This is the foundation for all other components of internal control providing discipline and structure for the business operations.

The VersaFile control environment establishes the basis for organizational processes, and influences control procedures and discipline of employees. Controls are designed to meet relevant trust criteria. The control environment at VersaFile begins with management's philosophy and operating style as well as the priorities and direction provided by the Executive Management team. The entire VersaFile organization is dedicated to delivering the highest level of customer service. The company has created a corporate culture that supports this mission.

Commitment to Integrity and Ethical Values

The effectiveness of controls cannot rise above the integrity and ethical values of the people, who create, administer, and monitor them. Integrity and ethical values are essential elements of the control environment, affecting the design, administration, and monitoring of other components. They include management's actions to remove or reduce incentives and temptations that might prompt personnel to engage in dishonest, illegal, or unethical acts. They also include the communication of entity values and behavioral standards to personnel through policy statements, codes of conduct, and leadership's example.

VersaFile understands the importance of integrity and ethical values and implements, maintains, and regularly communicates a code of conduct and other policies regarding acceptable business practices, guidance on conflicts of interest, and expected standards of ethical and moral behavior to all employees and contractors. VersaFile has formalized an equality and diversity policy that is available and acknowledged by all the employees.

In addition, VersaFile has established an employee handbook outlining requirements on the code of conduct, acceptable usage and confidentiality commitments which are reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions. Third-party contractors working on behalf of the organization are required to

sign an agreement outlining the standard code of conduct, security and confidentiality requirements.

Commitment to Competence

Competence is the knowledge and skills necessary to accomplish tasks that define the individual's job. Commitment to competence includes management's consideration of the competence levels for particular jobs and how those levels translate into requisite skills and knowledge.

VersaFile assigns job responsibilities to personnel based on knowledge and skills needed to adequately perform each job and has a process in place to evaluate the competency of employees on an annual basis. VersaFile reinforces these responsibilities by providing hands-on training during the initial period of employment, and continual hands-on training for new business processes or job responsibilities.

Management's Philosophy and Operating Style

Management's philosophy and operating style encompass a broad range of characteristics. Such characteristics may include the following: management's approach to taking and monitoring business risk; management's attitude and actions for the security and confidentiality of information.

The VersaFile management team is customer-driven and tightly focused on providing value to customers. Security is recognized as key components of the value proposition of the Managed Services and Technical Services offerings. Controls over Security are recognized as key enablers for delivery of value to the customer.

Executive Oversight & Assignment of Authority and Responsibility

The VersaFile Executive Team is ultimately accountable for oversight of VersaFile operations. The Executive Team meets on a monthly basis to provide oversight on internal controls, operations and business objectives supporting the VersaFile Services.

Management's policies and communications are directed at ensuring that 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.

Assignment of authority and responsibility includes delegation of authority to deal with organizational goals and objectives, operating functions and regulatory requirements,

including responsibility for information systems and authorizations for changes. To support this, management has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and operations of its services. The organization structure is reviewed and updated in case of significant changes. In addition, job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees and are reviewed and updated annually or in case of significant changes.

As mentioned above, VersaFile has defined job responsibilities and clear communication channels to disseminate information within the organization enabling VersaFile to react to market and regulatory changes and to meet its goals and objectives. VersaFile is appropriately staffed to support its operations, particularly with respect to critical areas such as software development, implementation, customer support, and information technology system support.

Human Resource Policies and Practices

HR policies and practices relate to hiring, orientation, training, evaluating, counseling, and remedial action. Standards for hiring qualified individuals with an emphasis on educational background, prior work experience, past accomplishments, evidence of integrity and ethical behavior demonstrate a commitment to maintaining the integrity of systems and data. All new employees and contractors are subjected to reference checks prior to joining the organization.

VersaFile maintains a commitment to hiring and retaining only highly competent and trustworthy people. Personal career growth and reward of meeting expectations are driven by periodic performance feedback and demonstrate VersaFile commitment to advance qualified personnel to higher levels of responsibility. Personnel who work for VersaFile are required to read and acknowledge the company's internal policies and confidentiality requirements as well as the confidentiality of customer managed information.

Risk Assessment

The VersaFile Executive Management team performs annual risk assessments, which requires VersaFile to identify risks in its areas of responsibility and to implement appropriate measures to address those risks. VersaFile management reevaluates the risk assessment at least annually to both update the previous results and to identify any new potential areas of concern. The risk assessment process assesses risks related to security,

fraud, regulatory and technology changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.

The risk assessment process consists of the following phases:

- Identifying – The identification phase includes listing out risks (including threats and vulnerabilities) that exist in the environment. This phase provides a basis for all other risk management activities.
- Assessing – The assessment phase considers the potential impact(s) of identified risks to the service organization and their likelihood of occurrence.
- Mitigating – The mitigation phase includes putting controls, processes, and other physical and virtual safeguards in place to prevent and detect both identified and assessed risks.
- Reporting – The reporting phase results in risk reports provided to managers with the necessary data to make effective business decisions and to comply with internal policies and any applicable regulations.
- Monitoring – The monitoring phase includes the performance of monitoring activities by VersaFile management team to evaluate whether the processes, initiatives, functions, and/or activities are mitigating the risk as designed.

Prior to engaging with new vendors and on an annual basis, management assesses the risk (and ongoing performance) of working with that vendor taking into account considerations such as the role of the vendor and their access to in-scope systems and data. A process is in place to remove access to systems and data when the vendor relationship has been terminated.

In-Scope Trust Service Categories

The table below provides the Trust Service Categories within the scope of this report. The controls designed and implemented to meet the applicable trust service criteria have been included in Section IV.

Trust Service Categories	Definition
Security	Information and systems are protected against unauthorized access, unauthorized disclosure of information, and damage to systems that could compromise the availability, integrity, confidentiality, and privacy of information or systems and affect VersaFile's ability to achieve its service commitments and system requirements.

Security

Security refers to the protection of:

i. Information during its collection or creation, use, processing, transmission, and storage and;
ii. Systems that use electronic information to process, transmit or transfer, and store information to enable the entity to meet its objectives. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft, or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Trust Service Criteria and Related Control Activities

Integration with Risk Assessment

Along with assessing risks, VersaFile management has identified and put into effect the necessary actions to address those risks. To address these risks, control activities have been placed into operation to help ensure that the actions are carried out in a competent and efficient manner. Control activities serve as mechanisms for managing the achievement of the Security categories and applicable criteria.

Selection and Development of Control Activities

The applicable trust criteria and related control activities are included in Section IV of this report, to eliminate the redundancy that would result from listing the items in this section as well. Although the control activities are included in Section IV, they are, nevertheless, an integral part of VersaFile description of its VersaFile Services. Any applicable TSC that are not addressed by control activities at VersaFile are also described within Section IV.

The description of the service auditors' tests of operating effectiveness and the corresponding results are also presented in the testing matrices, adjacent to the service organization's control procedures. The description and results of such tests are the responsibility of the service auditor and should be considered information provided by the service auditor.

Information and Communication

Information Systems

VersaFile Services are maintained in a virtualized environment on the chosen cloud platform. VersaFile relies on the applicable physical and logical security controls in place at the corresponding cloud platform facilities to ensure equipment and information is protected from unauthorized access.

Confidential data transmitted through the VersaFile Services are secured and protected using various access control and encryption technologies. Other information systems are used internally by VersaFile to communicate information throughout the organization, such as secure/encrypted email and manual or automated processes for recording and reporting internal decision support information.

Internal communication of information that supports internal controls

Management is involved with day-to-day operations and is able to provide personnel with an understanding of their individual roles and responsibilities. This includes the ability to provide necessary training to the extent that personnel understand how their daily activities and roles relate to the overall support of services. VersaFile management believes that open communication throughout the organization ensures that deviations from standards are identified, reported, and, appropriately addressed.

Internal policies and procedure documents relating to Security are maintained and made available to employees through the OneTrust platform and Microsoft 365.

External communication regarding internal controls

During the onboarding process, designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities. VersaFile has developed system documents and user guides that describe relevant system components as well as the purpose and design of the system. These documents are made available to internal and external users and updated on an as needed basis.

Customers are communicated on the Security commitments as part of terms of service which is required to be accepted by customers during initial access to the VersaFile Services. Any changes or Incidents that may affect the Security of the VersaFile Services are communicated to internal and external users, through system notifications that are advertised to platform users in advance of the planned changes.

Management strives to be proactive in responding to customer complaints and maintain a high level of inter-departmental communication about these events.

Control Activities

Identity and Access Management

Individual user accounts are required for user entities to access the VersaFile Services. These consist of all necessary account types to allow users to perform their essential roles and responsibilities. Each user account and associated username is unique and is identifiable to an individual user.

Privileged accounts i.e. the accounts that are required to access cloud platform production and non-production environments (including servers and databases), system administrator accounts and the administrator accounts required to manage the Platform, are only granted to a limited number of personnel based on job responsibilities after authorization from management.

For internal users that are required to access the Platform or supporting infrastructure, access rights are assigned by management based on the individual's role and responsibilities. Users with privileged access to the production environment or

generic/system administrator accounts are granted to a limited number of personnel and subject to a secondary level of authorization.

In order to detect misalignments in access rights, management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review and/or anytime a user's role changes. In addition, terminated internal users with access to VersaFile Services and supporting infrastructures are disabled or removed in a timely manner.

Authentication Management

VersaFile enforces access to the VersaFile Services and its supporting infrastructure through a combination of unique ID, strong password and multi-factor authentication mechanisms to production environments. Password standards have been established that define the appropriate password length, complexity and lockout threshold (as appropriate). These are enforced globally for all internal users and external users.

Platform Access

The VersaFile Platform is accessible to all approved user organizations and internal users and to meet the Security commitments, all client sessions to the VersaFile Services are encrypted through TLS/HTTPS. All sessions are logged and monitored, and the Firewall rules are reviewed on an annual basis.

VersaFile has implemented strong encryption technologies to protect communications and transmission of data. Confidential data transmitted through the VersaFile Services are secured and protected using various access control and encryption technologies.

Client Data Segregation

To ensure confidentiality of data within the VersaFile Services, customers are prevented from accessing other customers' data through appropriate segmentation controls. All customers receive their own logical tenant of the VersaFile Services and their data is logically separated and not accessible to other tenants to prevent unauthorized access. Data hosted and stored in databases and other storage locations is encrypted through the use of the cloud platform provided and managed encryption keys to encrypt data at rest.

Secure Data Disposal

VersaFile has defined policies that specify the data back-up and retention period, and process to follow for the secure disposal of confidential or sensitive information stored within the VersaFile Services. As part of the terms of service which are required to be accepted by customers during initial access to the VersaFile Services, specifics on the disposal and return of confidential information on termination or expiration of contract are included.

Workstation & Mobile Device Management

VersaFile utilizes a mobile device management solution to centrally configure, manage and monitor the compliance of company owned and BYOD devices with information security policies.

The standard protection suite for all corporate laptops and workstations includes:

- Anti-virus/anti-malware software configured to force updates to definitions on a minimum of a daily basis and to perform file-level scans during any read/write operations.
- Firewalls are enabled to prevent or detect unauthorized or malicious attempts to gain access to the device.
- Operating Systems are kept up to date with security updates being applied in an expedited manner.
- Disk encryption and passwords applied.

Change Management

For SaaS Solutions, VersaFile has developed a formal change management methodology that governs the development, acquisition, implementation, and maintenance of the VersaFile Services. For the VersaFile Services as applicable there are separate logical environments that are used to segregate access and between Development, Testing and Production instances. These environments are used to support a consistent code release and change management workflow in order to ensure product enhancements and bug fixes are efficiently and accurately reviewed, prioritized, scheduled, tested, signed-off and approved by senior management before being released into the production environment.

VersaFile has established a formal change management process that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed. In accordance with this process,

changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment and access to promote changes to production is restricted to authorized personnel based on job responsibilities.

Emergency changes may be necessary to repair, resolve or prevent a live operational issue that is impacting (or is about to impact) the business to a high degree and/or is to protect the organization from a threat and must be introduced as soon as possible.

VersaFile executes emergency change requests using the standard change management process but allows for the process to happen at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.

For customer-hosted options with VersFile providing Managed Services, VersaFile supports the client owned change management processes to adhere to client governed standards.

Data Backup and Recovery

Customer data and user activity are recorded within the VersaFile Services via cloud platform relational database services. Backups of databases, via cloud provider backup services, are maintained for redundancy.

Backup procedures are in place to help ensure that backup media is secure, available, and verified for the integrity of data to help ensure recovery in the event of a primary production system failure.

Daily incremental back-ups are performed. Backups are monitored for failure using an automated system. In addition, VersaFile performs backup restoration testing on an annual basis to test the integrity and completeness of back-up information. The incident management process is invoked for anomalies. Business continuity and disaster recovery plans have been developed and are tested annually. Test results are reviewed, and contingency plans are updated.

In those examples where VersaFile Services are conducted on customer infrastructure, customer data and user activity are recorded within VersaFile Services via virtual machine snapshots and database backups.

Incident Management and Resilience

Documented incident management and escalation policies and procedures are in place to guide users in identifying, reporting, investigating and resolving system failures, incidents, and other security related matters. These policies and procedures are available and communicated to internal personnel. A ticketing system is utilized to document incidents, responses, and resolution. Protocols are in place for communicating incidents to relevant parties on an as needed basis.

Business continuity and disaster recovery plans have been developed and are tested annually. Test results are reviewed, and contingency plans are updated.

Monitoring

The ongoing monitoring of the control environment is achieved through active, hands-on management, including regularly scheduled meetings to discuss business and operational issues. VersaFile utilizes a risk-based approach to monitor business units and other entities throughout the organization, ensuring that enterprise-wide risks are prioritized and addressed on a priority basis. Results from the risk assessment are documented in formal communications to Executive Management and other relevant parties as appropriate. Internal controls are periodically assessed during the year in addition to:

- Cloud monitoring tools: The Company uses native cloud monitoring tools, such as Azure Monitor, to collect and analyze metrics, logs, and events from its cloud resources and services. These tools enable the Company to monitor the health, performance, and utilization of its cloud infrastructure, as well as to detect and respond to anomalies, errors, and incidents. The Company also uses third-party cloud monitoring tools, such as Datadog to enhance its visibility and insights into its cloud environments and services. These tools provide additional features, such as dashboards, alerts, notifications, and reports, to help the Company manage and optimize its cloud operations.

- Security monitoring tools: The Company uses various security monitoring tools, such as Azure Security Center, to monitor and protect its cloud environments and services from threats and vulnerabilities. These tools provide continuous security assessment and detection, as well as recommendations and remediation actions, to help the Company improve its cloud security posture. The Company also uses third-party security monitoring tools, such as OpenVAS to perform vulnerability scanning, as well as to comply with security standards and regulations.

- Backup and recovery monitoring tools: The Company uses various backup and recovery monitoring tools, such as Azure Backup, to monitor and manage its backup and recovery processes and policies. These tools enable the Company to backup and restore its clients' data and applications in the cloud, as well as to ensure the availability and integrity of its backup and recovery solutions.

These tools automatically generate alerts for key activities that may require attention. Support teams are immediately notified of these alerts and they are actioned in a timely manner. System logs are retained for forensic purposes and interrogated as needed.

Complementary Subservice Organization Controls

VersaFile uses various cloud providers and customer-owned self-hosted infrastructure for the delivery of VersaFile Services. The cloud providers and the customers, as appropriate, are responsible for providing physical and environmental security controls, administration of their infrastructure, and for reporting any logical or physical security incidents.

Controls that VersaFile assumes will be implemented by applicable subservice organizations and customers and deemed to be high risk are evaluated through an assessment of the sub service organization's SOC or other relevant compliance report. VersaFile engages the customer for review of their security protocols when the customer is hosting the infrastructure directly. These evaluations consider the appropriateness of scope, impact of identified exceptions and the implementation of applicable complementary user entity controls.

VersaFile's controls related to the services in-scope cover only a portion of the overall internal control structure for each user entity of the in-scope services. It is not feasible for the control objectives related to the VersaFile Services to be achieved solely by VersaFile. Therefore, each user entity's internal controls must be evaluated in conjunction with VersaFile's controls described in Section IV of this report, taking into account the related complementary subservice organization controls (CSOCs) expected to be implemented at the subservice organization as described below.

Control Activities Expected to be Implemented by Subservice Organization	Service Provider	Applicable Trust Criteria
Service Provider is responsible for restricting logical and physical access to data center facilities, backup media, and other system components including firewalls, routers, and servers.	Microsoft Azure	CC6.1, CC6.2, CC6.3, CC6.4, CC6.5, CC6.6, CC6.7, CC6.8, CC9.2
Service Provider is responsible for identifying changes that could significantly impact the system of security controls, including the effects, both positive and negative, on its clients.	Microsoft Azure	CC3.4, CC8.1
Service Provider is responsible for implementing measures to prevent or mitigate threats consistent with their risk assessment.	Microsoft Azure	CC3.1, CC6.8, CC7.5, CC9.2
Service Provider is responsible for maintaining segregation of VersaFile's environment(s) from other Service Provider clients.	Microsoft Azure	CC6.1, CC6.6
Service Provider is responsible for managing and rotating the keys used to encrypt data at rest.	Microsoft Azure	CC6.1, CC6.6, CC6.7
Service Provider is responsible for managing encryption on all production databases and storage locations.	Microsoft Azure	CC6.1, CC6.6, CC6.7
Service Provider is responsible for maintaining the security and availability of the single sign on connection with the VersaFile Services.	Microsoft Azure	CC6.1
Service Provider is responsible for automatically scaling servers within the production environment.	Microsoft Azure	CC7.2

Service Provider is responsible for automatically scaling databases within the production environment.	Microsoft Azure	CC7.2
Service Provider is responsible for maintaining the integrity of system logs and their associated configurations.	Microsoft Azure	CC5.3, CC7.1, CC7.2
Service Provider is responsible for evaluating the impact of a security incident, remediating against incidents, and working towards prevention of future incidents.	Microsoft Azure	CC7.2, CC7.3, CC7.4, CC7.5
Service Provider is responsible for the management of any third-party vendors with access to customer environments.	Microsoft Azure	CC9.1

The full list of subservice organizations is described at the beginning of Section 3.

Complementary User Entity Controls

VersaFile's services were designed with the assumption that certain policies, procedures, and controls are implemented by its user entities (or customers). In certain situations, the application of specific policies, procedures, and controls by the customer is necessary to achieve the service commitments and system requirements that are based on the applicable trust services criteria included in this report. This section describes the additional policies, procedures, and controls customers may need to implement in order to satisfy the service commitments and system requirements for customers' specific use cases.

- Verifying the completeness and accuracy of data entered into the VersaFile Services.
- Immediately notifying VersaFile of incidents and actual or suspicious events or breaches in regards to security and availability, and providing assistance as necessary, to permit problem resolution.
- Attending training and reading product documentation on the functional use of the VersaFile Services and training end users on how to use the VersaFile Services.

- Reviewing and taking action upon notification of VersaFile's communication in regard to system changes, maintenance windows or other matters impacting VersaFile's service commitments.
- Processing data in accordance with their corporate confidentiality policies.
- Notifying VersaFile of any approved contact modifications. User entities should consider specifying one or more administrators who shall have the rights to authorize changes to their accounts.
- Monitoring the use of the VersaFile Services and the information contained therein to confirm that users are using the system and information for the right purpose.
- Confirming that end users are managing information from the VersaFile Services in accordance with their information security and other internal policies.
- Determining whether VersaFile's security infrastructure is appropriate for its needs and for notifying the service organization of any requested modifications.
- Maintaining the security, availability, and confidentiality of the devices used to connect to the VersaFile Services.
- Assigning usernames and passwords to authorized users, activating MFA if deemed necessary; and maintaining the confidentiality of login credentials.
- Periodically reviewing end users' access to the VersaFile Services for validity and appropriateness and making corrective changes within a timely manner.
- Ensuring that third-party integrations are active and working with any Client-provided credentials, in the instance where VersaFile is simply a pass-through enabler of data from said integrations.
- Restricting the transmission, movement, and removal of client information as needed and determining best practices in the creation and transmission of client data.
- Deploying security controls related to their operation to both protect against and detect security incidents, in addition to acting upon security incidents be it suspected or actual.
- Protecting confidential information within the boundaries of their systems.
- Notifying VersaFile of any changes to their confidentiality requirements and obtaining approval in writing.
- Maintaining their data in accordance with their own data retention and disposal policies and for notifying VersaFile of any such policies and procedures.
- Maintaining responsibility for the content uploaded to the VersaFile Services and ensuring that files are free from viruses and malware.

Section IV

Trust Service Criteria, Related Controls and Tests of Controls

Trust Service Criteria, Related Controls and Tests of Controls

Testing Approach

The objective of the auditor's controls testing is to determine the operating effectiveness of the controls specified by VersaFile's management throughout the examination period of April 1, 2023 to September 30, 2023. Testing was designed with the intent to perform procedures to provide reasonable but not absolute assurance that the specified controls were designed and operating effectively throughout the examination period, accounting for the evidence available.

Types of Tests Performed

1. Inquiry: tests include the corroboration of relevant personnel to verify the knowledge and understanding of the described control activity.
2. Observation: tests include the physical observation of the implementation, application of, or, existence of specific controls.
3. Inspection: tests include validating documents, records, configuration, or settings.
4. Re-performance: includes reprocessing transactions, procedures, & calculations to ensure the accuracy and completeness of the description.

Sampling Approach

The table below illustrates sampling that is utilized to determine the operating effectiveness of the controls specified by Appcues:

Control Type & Frequency	Minimum Number of Items to Test
Transaction / Occurrence based	10% up to 25
Manual control performed monthly	1-2
Manual control performed quarterly	1-2
Manual control performed annually	1
Application / Programmed control	1 application of each programmed control

Control Number	Description of VersaFile's Controls	Service Auditor Test	Test Results
Control Environment			
CC1.1 - COSO Principle 1: The entity demonstrates a commitment to integrity and ethical values.			
OM4	The organization has defined a Code of Conduct and Ethics and reviews them annually.	1. Inspect that the code of conduct has been reviewed within the past year.	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year. 2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook. 3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period.	No exceptions noted
OM9	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud,	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted

	harassment and other issues impacting the organization's ethical and integrity requirements.		
VM1	Third-party contractors/vendors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	1. For a sample of 3rd party vendors/contractors, inspect that they have signed their agreement to company's code of conduct, security and confidentiality requirements.	No occurrence of the control: Management represented that no third party contractors were onboarded during the audit period.
CC1.2 - COSO Principle 2: The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.			
VersaFile is a private company and does not have an independent Board of Directors. Executive Management is responsible for overseeing the strategic aspects of the company (including internal controls and compliance) as well as day to day operations.			
CC1.3 - COSO Principle 3: Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.			
HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities. 2. For a sample of new contractors,inspect that their employment agreement is signed and contains details of security responsibilities.	No exceptions noted

HR2	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	1. Inspect a sample of job descriptions for review in the past year and that it is stored in a location accessible to employees. 2. Inspect a sample of job descriptions and validate that it includes the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements.	No exceptions noted
HR3	Organization has established an organization chart that defines organizational roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services. The organization structure is reviewed and updated in case of significant changes.	1. Inspect that the current organization chart includes roles, reporting lines, and authorities as it relates to development, quality assurance, and security operations of its services and has been reviewed if any significant organization changes occurred during the audit period.	No exceptions noted
OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
CC1.4 - COSO Principle 4: The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.			

AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	1. Inspect information security policies for review by management within the past year. 2. Inspect that information security policies are posted on a platform that is accessible by employees	No exceptions noted
AT2	Employees are required to complete an information security and awareness training annually.	1. Inquire of management as to how security awareness training is conducted and attested to by employees. 2. For a sample of employees, inspect that they have completed training.	No exceptions noted
HR2	Job descriptions that document the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements are made available to the employees. Job descriptions are reviewed and updated annually or in case of significant changes.	1. Inspect a sample of job descriptions for review in the past year and that it is stored in a location accessible to employees. 2. Inspect a sample of job descriptions and validate that it includes the objectives of the role, responsibilities, reporting lines, employee qualifications and other requirements.	No exceptions noted
HR4	The organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	1. Inspect that a performance evaluation was performed in accordance with process for a sample of employees.	No exceptions noted

HR5	The organization has a formal training plan in place for the employees and meets annually to identify relevant training needs to support in scope-systems.	1. Inspect the annual training plan has been communicated to employees and reviewed within the past year	No exceptions noted
HR6	New employees and contractors are subjected to a background and reference checks prior to joining the organization.	1. Inspect that the employment hiring policy requires background/reference checks prior to new employees/contractors being hired. 2. For a sample of new employees/contractors, inspect evidence that background/reference check was performed.	No exceptions noted
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis. 2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.	No exceptions noted
CC1.5 - COSO Principle 5: The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.			

HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities. 2. For a sample of new contractors,inspect that their employment agreement is signed and contains details of security responsibilities.	No exceptions noted
HR4	The organization has a process in place to evaluate the competency of employees and identify their development needs on an annual basis.	1. Inspect that a performance evaluation was performed in accordance with process for a sample of employees.	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year. 2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook. 3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period.	No exceptions noted

OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.	No exceptions noted
OM9	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
Information and Communication			
CC2.1 - COSO Principle 13: The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.			
AT3	Designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	1. Inspect that the onboarding process includes functional training for customer focused employees. 2. Inspect that new customers are trained on the relevant applications	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within	No exceptions noted

	annual basis and identified deficiencies are remediated in a timely manner.	the last 12 months, identification of exceptions, and evidence of remediation.	
CC2.2 - COSO Principle 14: The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.			
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	1. Inspect information security policies for review by management within the past year. 2. Inspect that information security policies are posted on a platform that is accessible by employees	No exceptions noted
AT2	Employees are required to complete an information security and awareness training annually.	1. Inquire of management as to how security awareness training is conducted and attested to by employees. 2. For a sample of employees, inspect that they have completed training.	No exceptions noted
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	1. For a sample of system changes, inspect that the functionality and/or security changes were communicated (e.g. release notes) to affected parties in accordance with the change management process.	No exceptions noted

HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities. 2. For a sample of new contractors,inspect that their employment agreement is signed and contains details of security responsibilities.	No exceptions noted
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
OM5	The organization has established an employee Handbook outlining requirements on the Code of Conduct, acceptable usage and confidentiality commitments which is reviewed/updated on an annual basis by executive management. All employees are required to sign off on acceptance and acknowledgement of the employee handbook as part of the formal onboarding process and to re-sign in the event of any significant revisions.	1. Inspect that the employee handbook includes components of code of conduct, acceptable use and confidentiality responsibilities and has been reviewed by management within the past year. 2. For a sample of employees hired during the period, inspect that they have signed-off on the handbook. 3. For a sample of existing employees inspect that they have signed off on the handbook where significant revisions were made to the handbook during the period.	No exceptions noted

OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
OM9	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
VM1	Third-party contractors/vendors working on behalf of the organization are required to sign an agreement outlining the standard code of conduct, security and confidentiality requirements.	1. For a sample of 3rd party vendors/contractors, inspect that they have signed their agreement to company's code of conduct, security and confidentiality requirements.	No occurrence of the control: Management represented that no third party contractors were onboarded during the audit period.
CC2.3 - COSO Principle 15: The entity communicates with external parties regarding matters affecting the functioning of internal control.			
AT3	Designated customer administrators and relevant organizational employees are trained on the functional use of the application to understand their roles and responsibilities as part of the onboarding process.	1. Inspect that the onboarding process includes functional training for customer focused employees.	No exceptions noted

		2. Inspect that new customers are trained on the relevant applications	
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	1. For a sample of system changes, inspect that the functionality and/or security changes were communicated (e.g. release notes) to affected parties in accordance with the change management process.	No exceptions noted
HR1	Information security roles and responsibilities of employees, contractors, and the organization are stated in contractual agreements.	1. For a sample of new employees, inspect that their employment agreement is signed and contains details of security responsibilities. 2. For a sample of new contractors,inspect that their employment agreement is signed and contains details of security responsibilities.	No exceptions noted
IM1	The organization provides an external-facing support system that allows users to report incidents, complaints, issues, and any other challenge through an appropriate channel. Reported incidents are addressed by the organization's support staff in a timely manner.	1. Inquire of management as to how customer issues are recorded and actioned. 2. For a sample of customer issues, inspect that the issue was assigned and resolved (if applicable) in a timely manner.	No exceptions noted
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted

	process document is reviewed by management on an annual basis and updated as required.		
OM7	The organization has formal agreements in place with customers which acknowledges their compliance on security, confidentiality and privacy commitments.	1. For a sample of customers, inspect that the customer has signed their agreement to the company's security, confidentiality and privacy commitments.	No exceptions noted
OM9	The organization has established communication channels that allow employees to securely and anonymously report issues related to fraud, harassment and other issues impacting the organization's ethical and integrity requirements.	1. Inspect that the company has communicated the existence of a secure reporting channel to all employees.	No exceptions noted
OM10	New customer contracts or modifications to existing customer contracts and end-user license agreements (EULA) are reviewed annually by Management to ensure security and confidentiality commitments are met.	1. Inspect that the templates (specifically the security and/or confidentiality clauses) used for customer agreements have been reviewed by management within the past 12 months.	No exceptions noted
Risk Assessment			
CC3.1 - COSO Principle 6: The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year.	No exceptions noted

	documented and implemented by the organization's executive management.	2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	
CC3.2 - COSO Principle 7: The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year. 2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis. 2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.	No exceptions noted
CC3.3 - COSO Principle 8: The entity considers the potential for fraud in assessing risks to the achievement of objectives.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year.	No exceptions noted

	documented and implemented by the organization's executive management.	2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	
CC3.4 - COSO Principle 9: The entity identifies and assesses changes that could significantly impact the system of internal control.			
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year. 2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis. 2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.	No exceptions noted
Monitoring Activities			
CC4.1 - COSO Principle 16: The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.			
OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal	No exceptions noted

	to internal controls and delivery on key performance metrics.	controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.	No exceptions noted
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner.	No exceptions noted
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
CC4.2 - COSO Principle 17: The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.			
OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance),	No exceptions noted

	to internal controls and delivery on key performance metrics.	delivery on key performance metrics and actions agreed to by the executives were discussed.	
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.	No exceptions noted
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner.	No exceptions noted
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
Control Activities			
CC5.1 - COSO Principle 10: The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.			

OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.	No exceptions noted
CC5.2 - COSO Principle 11: The entity also selects and develops general control activities over technology to support the achievement of objectives.			
OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within	No exceptions noted

	annual basis and identified deficiencies are remediated in a timely manner.	the last 12 months, identification of exceptions, and evidence of remediation.	
CC5.3 - COSO Principle 12: The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.			
AT1	The organization utilizes Tugboat Logic platform to manage its Information Security policy and procedures. Internal policy and procedure documents relating to security, confidentiality, and availability are maintained and made available to employees. The policies and procedure documents are reviewed and approved by management annually or during significant changes.	1. Inspect information security policies for review by management within the past year. 2. Inspect that information security policies are posted on a platform that is accessible by employees	No exceptions noted
OM6	The organization's executive team meets on a monthly basis to discuss operations, issues relating to internal controls and delivery on key performance metrics.	1. For a sample of executive team meetings, inspect the minutes for evidence that operations, issues relating to internal controls (including security and compliance), delivery on key performance metrics and actions agreed to by the executives were discussed.	No exceptions noted
OM8	The organization uses Tugboat Logic to document their internal controls and continuously monitor its effectiveness. An assessment over the effectiveness and efficiency of the internal controls, processes and policies is reviewed by management on at least an annual basis and identified deficiencies are remediated in a timely manner.	1. Inquire of management as to how internal controls are periodically assessed. 2. Inspect the internal controls assessment document for performance/sign-off within the last 12 months, identification of exceptions, and evidence of remediation.	No exceptions noted

Logical and Physical Access			
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.			
AA1	Unique user IDs and strong passwords are required in order to gain access to the infrastructure supporting the application (i.e. Active Directory, server and database accounts).	1. Inspect the password parameters for each in scope infrastructure element and validate they align to the control description.	No exceptions noted
AA2	Unique user IDs and strong passwords are required in order to gain access to the application production environment.	1. Inspect the password parameters for each in scope application and validate they align to the control description.	No exceptions noted
AA3	Multi-factor authentication (MFA) is enforced for user accounts with administrative access to the organization's production platform.	1. Inspect authentication parameters and validate that Multi Factor Authentication is required for admin/generic access to production.	No exceptions noted
AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems. 2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.	No exceptions noted

AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	1. Inquire of management as to the access management procedures performed to remove access for terminated individuals. 2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.	No exceptions noted
AC5	System components are configured such that the organization and its customers' access is appropriately segmented from other tenant users.	1. Inquire of management as to how customer data is segmented within the applications and databases. 2. Inspect system configuration settings and validate that they restrict access to customer data.	No exceptions noted
OM1	The organization maintains an inventory of production information assets including details on asset ownership, data classification and location. The asset inventory listing is reviewed and updated by management on an as-needed basis.	1. Inspect the IT asset inventory document includes details on asset ownership, data classification and location; and that it has been reviewed and approved within the last 12 months.	No exceptions noted
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy.	No exceptions noted

		2. Inspect that the individuals with access to encryption keys are authorized.	
SO5	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	1. Inquire of management as to what tools are used to ensure data in databases is encrypted. 2. Inspect system configurations for evidence that data at rest is encrypted.	No exceptions noted
SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	1. Inquire of management as to what tools are used to ensure data in transit is encrypted. 2. Inspect system configurations for evidence that data in transit is encrypted.	No exceptions noted
SO11	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	1. Inspect the network diagram for description of protection mechanisms in place. 2. Inspect the network diagram for review within the past year.	No exceptions noted
CC6.2 - Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.			

AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems. 2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.	No exceptions noted
AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	1. Inquire of management as to the access management procedures performed to remove access for terminated individuals. 2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.	No exceptions noted
AC4	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	1. Select a sample of user reviews and inspect for evidence of review, sign-off and remediation.	No exceptions noted
CC6.3 - The entity authorizes, modifies, or removes access to data, software, functions, and other protected information assets based on roles, responsibilities, or the system design and changes, giving consideration to the concepts of least privilege and segregation of duties, to meet the entity's objectives.			

AC1	Access to in-scope system components (application(s) and its underlying infrastructure) requires a documented access request and approval from management prior to access provisioning.	1. Inquire of management as to the access management policy, procedures performed and individuals authorized to grant access to systems. 2. For a sample of new users, inspect the access request document and validate that approval was obtained from an authorized individual prior to access being provisioned on the system.	No exceptions noted
AC2	Management utilizes an employee termination checklist to ensure that the termination process is consistently executed and access is revoked for terminated employees in a timely manner.	1. Inquire of management as to the access management procedures performed to remove access for terminated individuals. 2. For a sample of terminated employees, inspect that a termination checklist documenting all logical access removed was completed and approved by management and that logical access was removed from the systems in a timely manner.	No exceptions noted
AC3	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	1. Inquire of management as to the process for managing access privilege/administrative accounts (end user, generic and system/service) accounts on the in-scope servers and databases. 2. Inspect list of all administrative/privilege accounts on the in- scope systems to determine that access to these accounts are	No exceptions noted

		restricted to authorized and appropriate personnel.	
AC4	Management performs a quarterly user access review for in-scope system components to ensure that access is restricted appropriately. Access is modified or removed in a timely manner based on the results of the review.	1. Select a sample of user reviews and inspect for evidence of review, sign-off and remediation.	No exceptions noted
AC6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	1. Inspect that the deployment tool is configured to restrict whom has access to deploy changes into the production environment. 2. Inspect that mandatory code review by an individual other than the developer is required prior to deploying into production.	No exceptions noted
CC6.4 - The entity restricts physical access to facilities and protected information assets (for example, data center facilities, back-up media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.			
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
CC6.5 - The entity discontinues logical and physical protections over physical assets only after the ability to read or recover data and software from those assets has been diminished and is no longer required to meet the entity's objectives.			

DS4	Formal data retention and disposal procedures are in place to guide the secure retention and disposal of information.	1. Inspect that data retention & disposal policies and procedures are in place and approved by management. 2. Inspect one example of data being disposed in accordance with procedure.	No occurrence of the control: Management represented that Sharepoint sites and Microsoft 365 are configured to retain data permanently. Hence no data was deleted during the audit period.
CC6.6 - The entity implements logical access security measures to protect against threats from sources outside its system boundaries.			
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy. 2. Inspect that the individuals with access to encryption keys are authorized.	No exceptions noted
SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	1. Inquire of management as to what tools are used to ensure data in transit is encrypted. 2. Inspect system configurations for evidence that data in transit is encrypted.	No exceptions noted

SO11	A formal network diagram outlining boundary protection mechanisms (e.g. firewalls, IDS, etc.) is maintained for all network connections and reviewed annually by IT management.	1. Inspect the network diagram for description of protection mechanisms in place. 2. Inspect the network diagram for review within the past year.	No exceptions noted
SO15	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.	1. Inspect that firewall rules are configured on the application gateway and production network and have been reviewed within the past year.	No exceptions noted
CC6.7 - The entity restricts the transmission, movement, and removal of information to authorized internal and external users and processes, and protects it during transmission, movement, or removal to meet the entity's objectives.			
SO4	The organization uses its cloud provider key management service to encrypt data at rest and to store and manage encryption keys. Access to production access keys is restricted to authorized individuals.	1. Inspect the encryption and key management policy and validate that key management system is used in accordance with policy. 2. Inspect that the individuals with access to encryption keys are authorized.	No exceptions noted
SO5	Customer data is encrypted at rest (stored and backup) using strong encryption technologies.	1. Inquire of management as to what tools are used to ensure data in databases is encrypted. 2. Inspect system configurations for evidence that data at rest is encrypted.	No exceptions noted

SO6	Encryption technologies are used to protect communication and transmission of data over public networks and between systems.	1. Inquire of management as to what tools are used to ensure data in transit is encrypted. 2. Inspect system configurations for evidence that data in transit is encrypted.	No exceptions noted
CC6.8 - The entity implements controls to prevent or detect and act upon the introduction of unauthorized or malicious software to meet the entity's objectives.			
AC3	Access to a generic administrator or privileged accounts on the databases and servers supporting the application is restricted to authorized personnel based on a role-based access scheme.	1. Inquire of management as to the process for managing access privilege/administrative accounts (end user, generic and system/service) accounts on the in-scope servers and databases. 2. Inspect list of all administrative/privilege accounts on the in- scope systems to determine that access to these accounts are restricted to authorized and appropriate personnel.	No exceptions noted
CM1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.	1. Inspect that the change management process was reviewed by IT management within the past year.	No exceptions noted
SO1	Antivirus software is in place to prevent or detect and act upon the introduction of unauthorized or malicious software.	1. Inquire of management of Antivirus policy and the systems where Antivirus applies.	No exceptions noted

		2. Inspect the Antivirus software configuration and validate it is set to perform real time file-level scans and program/definition updates at least daily.	
System Operations			
CC7.1 - To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.			
SO9	A log management process has been formalized to make sure that access to change the log configuration and access to modify logs is restricted.	1. Inquire of management as to the log management process (configuration & retention). 2. Inspect the log configuration and validate that only authorized individuals have access to modify the log settings and the log files.	No exceptions noted
SO14	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	1. Inspect logging configurations and validate that key activities are included. 2. Inspect notification/alert settings and validate that alerts are enabled for all key activities and personnel set up to receive alerts are appropriate. 3. Inquire of management for how anomalies detected are investigated and resolved.	No exceptions noted
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the	1. For a sample of vulnerability scans, inspect that scope of the scan was	No exceptions noted

	production systems. Issues identified are analyzed and remediated in a timely manner.	documented and that issues are analyzed and remediated in a timely manner.	
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.			
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No exceptions noted
SO14	Logging is enabled to monitor activities such as administrative activities, logon attempts, changes to functions, security configurations, permissions, and roles. Automated alerts are configured to notify IT management and issues identified are resolved in a timely manner through the incident management process.	1. Inspect logging configurations and validate that key activities are included. 2. Inspect notification/alert settings and validate that alerts are enabled for all key activities and personnel set up to receive alerts are appropriate.	No exceptions noted

		3. Inquire of management for how anomalies detected are investigated and resolved.	
SO15	System firewalls are configured on the application gateway and production network to limit unnecessary ports, protocols and services. Firewall rules are reviewed on an annual basis by IT management.	1. Inspect that firewall rules are configured on the application gateway and production network and have been reviewed within the past year.	No exceptions noted
SO16	IT team continuously monitors system capacity and performance through the use of monitoring tools to identify and detect anomalies that could compromise availability of the system operations. Incident management process is invoked for confirmed events and anomalies.	1. Inspect logging configurations and validate that performance related measures are included. 2. Inspect notification/alert settings and validate that alerts are enabled for all key measures and personnel set up to receive alerts are appropriate. 3. For a sample of alerts, inspect back-up documentation and validate that actions were taken to resolve the issue in accordance with log management process.	No exceptions noted
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.			
IM2	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable timeframe to meet the organization's privacy and confidentiality commitments.	1. Inspect that the incident management process contains details of notifying affected parties in case of a data breach. 2. For a sample of data breaches, inspect that notification was provided to affected	No exceptions noted

		parties in accordance with incident management process.	
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No exceptions noted
IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	1. Inspect that incident management process contains details of performing a post-mortem on closed incidents. 2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed.	No exceptions noted
CC7.4 - The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.			

CR2	Weekly full-system and daily incremental backups are performed using an automated system and replicated to offsite location. Backups are monitored for failure using an automated system.	1. Inspect the backup schedule and configuration on the backup tool and confirm that the system is configured for taking weekly full and daily incremental backups of the application and databases. 2. Inspect backup system configuration and confirm that data backups are replicated to an offsite location. 3. Inspect backup configuration and confirm that the system is setup to notify the relevant personnel in the event of failures and that the persons set up to receive the notifications have responsibilities over the backup process. 4. For a sample of backup failures, inspect evidence that failures were resolved within a timely manner.	No exceptions noted
CR6	Disaster recovery plans (including restoration of backups) have been developed and tested annually. Test results are reviewed and consequently contingency plans are updated.	1. Inspect the DRP for management review within the last year. 2. Inspect test results for evidence of review and follow-up.	No exceptions noted
IM2	Notifications regarding confirmed data breaches are provided to affected data subjects, regulators, and other parties (as applicable) within an acceptable	1. Inspect that the incident management process contains details of notifying affected parties in case of a data breach.	No exceptions noted

	timeframe to meet the organization's privacy and confidentiality commitments.	2. For a sample of data breaches, inspect that notification was provided to affected parties in accordance with incident management process.	
IM3	A formal incident management process has been established and implemented which requires incidents to be tracked, documented and resolved in a complete, accurate and timely manner. The process document is reviewed by management on an annual basis and updated as required.	1. Inspect that the incident management process contains key elements and has been reviewed by management within the past year.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No exceptions noted
IM5	Management has established defined roles and responsibilities to oversee implementation of security policies including incident response.	1. Inspect the Information Security policy (and Incident Management process if necessary) for defined roles and responsibilities for implementing and operating key security functions (including incident response).	No exceptions noted

IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	1. Inspect that incident management process contains details of performing a post-mortem on closed incidents. 2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed.	No exceptions noted
SO17	Vulnerability scan is performed on a quarterly basis to identify threats and vulnerabilities to the production systems. Issues identified are analyzed and remediated in a timely manner.	1. For a sample of vulnerability scans, inspect that scope of the scan was documented and that issues are analyzed and remediated in a timely manner.	No exceptions noted
CC7.5 - The entity identifies, develops, and implements activities to recover from identified security incidents.			
CR6	Disaster recovery plans (including restoration of backups) have been developed and tested annually. Test results are reviewed and consequently contingency plans are updated.	1. Inspect the DRP for management review within the last year. 2. Inspect test results for evidence of review and follow-up.	No exceptions noted
IM4	All incidents related to security are logged, tracked and communicated to affected parties. Incidents are resolved in a timely manner in accordance with formal incident management process.	1. Inquire of management and inspect the incident management process for how incidents are logged, communicated and resolved. 2. For a sample of incidents during the period, inspect that the incidents were analyzed, communicated and resolved according to the process.	No exceptions noted

IM6	Management incorporates lessons learned from ongoing incident response activities into incident response procedures on an ongoing basis.	1. Inspect that incident management process contains details of performing a post-mortem on closed incidents. 2. For a sample of incidents, inspect the incident response documentation for evidence of a post-mortem being performed.	No exceptions noted
SO12	A patch management process exists to confirm that operating system level vulnerabilities are remediated in a timely manner. In addition, production servers are scanned to test patch compliance on a quarterly basis.	1. Inspect the patch management process and validate that operating system vulnerabilities are addressed in a timely manner. 2. For a sample of quarterly scan results on production servers, inspect the results to validate management has assessed the level of compliance.	No exceptions noted
Change Management			
CC8.1 - The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.			
AC6	Access to promote changes to production is restricted to authorized personnel based on job responsibilities.	1. Inspect that the deployment tool is configured to restrict whom has access to deploy changes into the production environment. 2. Inspect that mandatory code review by an individual other than the developer is required prior to deploying into production.	No exceptions noted

CM1	A formal change management process exists that governs changes to the applications and supporting infrastructure. The process document is reviewed by IT management on an annual basis and updated as needed.	1. Inspect that the change management process was reviewed by IT management within the past year.	No exceptions noted
CM2	Emergency change requests are documented and subject to the standard change management process but at an accelerated timeline. Prior to initiating an emergency change, appropriate approval is obtained and documented.	1. For a sample of emergency system changes made during the year, inspect that the changes were documented, tested and approved prior to implementation and in accordance with the change management process.	No exceptions noted
CM4	Changes that affect the functionality and security of the system components are communicated to internal and external users.	1. For a sample of system changes, inspect that the functionality and/or security changes were communicated (e.g. release notes) to affected parties in accordance with the change management process.	No exceptions noted
CM5	Changes to the application(s) and supporting infrastructure are documented, tested and approved by authorized personnel prior to implementation into the production environment in accordance with the change management process.	1. For a sample of system changes made during the year, inspect that the changes were documented, tested and approved prior to implementation and in accordance with the change management process.	No exceptions noted
CM6	Changes to application and system infrastructure are developed and tested in a separate development or test environment before implementation.	1. For a sample of changes to the production environment, inspect change documentation and validate that the changes were tested in a segregated environment.	No exceptions noted
Risk Mitigation			

CC9.1 - The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.			
RM1	Management maintains insurance coverage through an external service provider against major financial risks for overall business.	1. Inspect that an insurance certificate/policy exists with a 3rd party that covers major financial risks.	No exceptions noted
RM2	Management performs a formal risk assessment process (which includes risks related to security, fraud, regulatory and technology changes) on an annual basis or in the event of significant changes. Identified risks along with mitigation strategies are documented and implemented by the organization's executive management.	1. Inspect that a risk assessment exists and has been updated and reviewed within the past year. 2. Inspect the risk assessment for acknowledgement of security/technology related risks and mitigation strategies.	No exceptions noted
CC9.2 - The entity assesses and manages risks associated with vendors and business partners.			
VM2	On an annual basis, management performs reviews of SOC reports from service providers/vendors to review the appropriateness of scope, impact of identified exceptions and applicable complementary user entity controls.	1. Inspect that SOC reports for key vendors have been reviewed by management with impacts of exceptions analyzed, follow-ups performed with vendor where necessary and complementary user entity controls identified where applicable.	No exceptions noted
VM3	A vendor management process has been implemented whereby management performs risk assessments of potential new vendors and evaluates the performance of existing vendors on an annual basis. Corrective actions are taken as required based on the results of the assessments.	1. Inspect that the vendor management process includes performance of risk assessments for new and existing vendors on at least an annual basis. 2. For a sample of vendors, inspect that a risk assessment was performed with required actions taken.	No exceptions noted

VM4	Vendor management process has been implemented that includes security procedures to be followed in case of vendor terminations.	1. Inspect that the vendor management process includes security procedures in the event agreements are terminated (e.g. data destruction or recovery, separation of APIs, etc). 2. For a sample of vendor terminations, confirm that access to programs and/or data was removed per the process	No exceptions noted