Sayers Technology Holdings, Inc.

Sayers Technology Services, LLC

Sayers Technology, LLC

Type II System and Organization Controls Report (SOC 2)

Report on a Service Organization's Description of Its System and on the Suitability of the Design and Operating Effectiveness of Its Controls Relevant to Security, Availability, and Confidentiality Throughout the Period August 1, 2024, to July 31, 2025.

Table of Contents

Section I:

Assertion of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC Management

Assertion of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC Management

We have prepared the accompanying description in section III titled "Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's Description of Its Personalized Hardware and Software Services System" throughout the period August 1, 2024, to July 31, 2025, (description), based on the criteria for a description of a service organization's system in DC section 200, *2018 Description Criteria for a Description of a Service Organization's System in a SOC 2 Report* (AICPA, *Description Criteria*), (description criteria). The description is intended to provide report users with information about the personalized hardware and software services system that may be useful when assessing the risks arising from interactions with Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's system, particularly information about system controls that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC has designed, implemented, and operated to provide reasonable assurance that its service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC use the following subservice organizations:

- Salesforce for cloud-based customer relationship management services
- Smartsheet for collaboration and work management services
- Microsoft for cloud computing services
- Rapid7 for threat detection services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC, to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC'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 operating effectively are necessary, along with controls at Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC, to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the

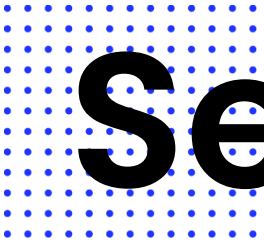
applicable trust services criteria. The description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls.

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

a. the description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system that was designed and implemented throughout the period August 1, 2024, to July 31, 2025, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period, and if the subservice organizations and user entities applied the complementary controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC'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 Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls operated effectively throughout that period.



Section II:

Independent Service Auditor's Report

Independent Service Auditor's Report

Chris Callahan
President and CEO
Sayers Technology, LLC
960 Woodlands Parkway
Vernon Hills, IL 60061

Scope

We have examined Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's accompanying description in section III titled "Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's Description of Its Personalized Hardware And Software Services System" throughout the period August 1, 2024, to July 31, 2025, (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 August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements were achieved based on the trust services criteria relevant to security, availability, and confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*).

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC uses the following subservice organizations:

- Salesforce for cloud-based customer relationship management services
- Smartsheet for collaboration and work management services
- Microsoft for cloud computing services
- Rapid7 for threat detection services

The description indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC, to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC'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 organizations, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

The description indicates that complementary user entity controls that are suitably designed and operating effectively are necessary, along with controls at Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC, to achieve Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements based on the applicable trust services criteria. The description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls, the applicable trust services criteria, and the complementary user entity controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls. Our examination did not include such complementary user entity controls and we have not evaluated the suitability of the design or operating effectiveness of such controls.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

Our responsibility is to express an opinion on the description and on the suitability of design and operating effectiveness of controls stated in the description based on our examination. Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether, in all material respects, the description is presented in accordance with the description criteria and the controls stated therein were suitably designed and operated 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 or did not operate effectively
- 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

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

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

Inherent Limitations

The description is prepared to meet the common needs of a broad range of report users and may not, therefore, include every aspect of the system that individual 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 provide reasonable assurance that the service organization's service commitments and system requirements are achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the suitability of the design or operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with policies or procedures may deteriorate.

Description of Tests of Controls

The specific controls we tested and the nature, timing, and results of those tests are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," of this report in columns 2, 3, and 4, respectively.

Opinion

In our opinion, in all material respects,

a. the description presents Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system that was designed and implemented throughout the period August 1, 2024, to July 31, 2025, in accordance with the description criteria.

b. the controls stated in the description were suitably designed throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's service commitments and system requirements would be achieved based on the applicable trust services criteria, if its controls operated effectively throughout that period and if the subservice organizations and user entities applied the complementary controls assumed in the design of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls throughout that period.

c. the controls stated in the description operated effectively throughout the period August 1, 2024, to July 31, 2025, to provide reasonable assurance that Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC'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 Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's controls operated effectively throughout that period.

Restricted Use

This report, including the description of tests of controls and results thereof in section IV, is intended solely for the information and use of Sayers, user entities of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's personalized hardware and software services system during some or all of the period August 1, 2024, to July 31, 2025, business partners of Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC subject to risks arising from interactions with the personalized hardware and software services system, practitioners providing services to such user entities and business partners, prospective user entities and business partners, and regulators who have sufficient knowledge and understanding of the following:

- The nature of the service provided by the service organization
- How the service organization's system interacts with user entities, business partners, subservice 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.

Joseph Kirkpatrick
CPA, CISSP, CGEIT, CISA, CRISC, QSA
4235 Hillsboro Pike, Suite 300
Nashville, TN 37215

August 29, 2025

Section III:

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC & Sayers Technology, LLC's Description of Its Personalized Hardware and Software Services System

Services Provided

Sayers Technology Holdings, Inc., Sayers Technology Services, LLC, and Sayers Technology, LLC (collectively "Sayers") is a managed services provider that offers three categories of service:

- NexGen Firewall Lifecycle Services: A continuous, four-phase firewall lifecycle management service. Customers and Sayers co-manage the firewalls, and customers can select from a menu of services to offload responsibilities to Sayers, including patching, upgrades, security reviews, and design services. Customers receive reports on best practice assessments, policy and rule reviews, and monthly and quarterly environment reviews.
- Azure Cloud Services: Sayers is a Microsoft Cloud Solutions Provider and resells Azure services to customers. The Cloud Architecture team conducts monthly check-in calls with customers.
- Staff Augmentation: Customers look to Sayers as a trusted technology partner, including staff augmentation services to fill critical roles on a stop-gap basis. An on-staff recruiting team finds qualified candidates, which are interviewed and assessed by engineers, for six-to-12-month contracts. These contracts are not project-based and define, in general, expected tasks. Candidates filling these roles may be employees or contractors and report to and are managed by the customer.
- Professional Services: Project-based professional services are offered; these projects are mainly driven by the three previous services.

Marketing and Sales

Sayers' internal Marketing team uses the Sayers website, social media, email campaigns, industry events, and word of mouth to advertise. Marketing efforts are coordinated through HubSpot. HubSpot is integrated into Salesforce; leads are tracked as opportunities. Leads are then routed to the appropriate representative based on who the account is assigned to.

Sales representatives contact leads hold high-level discussions about each lead's organization and the problem to be solved. Potential solutions are proposed to leads, and a member of the Services team assigns an engineer or other technical resource to participate in additional calls with the potential client in order to refine Sayers' understanding of the problem and propose a solution and implementation plan.

Information from calls is used to create a Green Light Document (GLD). GLDs are used to confirm the scope of the engagement, services to be provided, and a cost estimate. Approved GLDs are used to create formal Statements of Work (SOWs). SOWs are created from a template but are bespoke for the proposed solution specific to the client. SOWs include an executive summary of the services to be provided followed by a high-level phased implementation plan, a staffing plan, customer responsibilities and prerequisites, and itemized costs. SOWs are sometimes accompanied by a Sayers Master Services Agreement (MSA) that identifies Sayers' commitment to performance, assumption of risk of damages or injuries from providing services, reputable personnel with clear background checks and 10-panel drug testing, non-disclosure of sensitive

information, and information security controls. SOWs are presented by the sales representative and engineer to the client. SOWs, MSAs, and mutual non-disclosure agreements (mNDAs) are signed by clients using DocuSign upon the start of an engagement and are returned to Sayers.

Project Setup

Signed agreements are stored by the Services team in a shared network folder and are submitted to the Project Management team by completing a Smartsheet-based client intake form. The form's fields are completed by Services and are used to populate a Smartsheet spreadsheet and to generate a Smartsheet alert to the Project Management team of a new project to be assigned. Information transferred to Project Management includes the SOW, rates, and assigned resources. A Project Manager is assigned based on availability and creates Smartsheet documents from templates including the project plan, status template, project & client dashboard, and project finance sheet used to track invoicing as defined in the SOW. The project plan is populated based on the scope and phased steps identified in the SOW; project plans track: Tasks/Milestones, Notes, Start/End Dates, and Status by Phases including Planning, Prerequisite, and Implementation. Data in the project plan is used to populate two dashboards: Project and Client.

Project Dashboards are internal, with access limited to the Sayers team. Information displayed in project dashboards includes project metrics (status, start date, target end date, and days open); project budget (scoped project hours, approved change order hours, total project hours, total hours approved and invoiced, and remaining hours); project information (project number, salesforce opportunity number, primary customer contact & email, project manager & project engineer), and tasks/milestones (summary, status, start date, notes, health, duration (days), and latest comment.

Client Dashboards are client-facing and are limited to project information (project manager, primary engineer, account executive); project status (project health, start & target end dates), and project plan (tasks/milestones, status, start date, notes, health, duration).

Kickoff and Implementation

The Project Manager creates a draft kickoff presentation that is reviewed during the internal kickoff meeting, held as a team prior to meeting with the client to review the external kickoff draft. The meeting is attended by the Sales Representative, Services Director, Project Manager, and Delivery Engineers. The external kickoff meeting occurs with the client, and topics discussed include the project scope, deliverables, timeline, prerequisites, how often status calls will occur (if there will be status calls), and if any working sessions will be scheduled. A folder is created in ShareFile and is shared with the client contact and internal staff assigned to the project; this folder is used to securely share files between the client and Sayers. These files may include network diagrams and configuration information. Credentials provided by clients are stored in the Software-as-a-Service (SaaS)-based privileged access manager (PAM) Keeper. Access to client credentials is limited to engineers assigned to the client project.

Changes to SOWs are addressed through change orders. Clients use the Change Order form, included as an appendix to the SOW, to submit changes to their project manager. The Project Manager discusses submitted changes at the next internal check-in and presents a formal change to the client to sign and approve. Changes are tracked in project plans and are reflected in project information tracked in project dashboards.

When client dashboards are created, the client's project sponsors are invited by Project Management via Smartsheet email notification to register themselves and configure multi-factor authentication (MFA) to access the client dashboard. Clients can use this dashboard for the duration of a project for updates on tasks or milestones and any that are awaiting action. Project managers meet internally with engineers weekly to review project plans and dashboards; the Project Manager reviews the client dashboard with the client during status meetings. Progress in the project plan is updated by the Project Manager as tasks are reported as complete until completion. Project health is tracked on dashboards to represent an overall score of project progress.

Project Completion

Closeout calls are held both internally and externally. Internal calls are used to review the success of the project, lessons learned, and opportunities for additional business. Optional external calls are held with clients to review the success of the project and a review of deliverables. Clients are presented with a Certificate of Completion to sign. Upon signature of the certificate or following five days with no response, the project is closed. Upon project completion, ShareFile folders used for information transfer are marked for deletion and are automatically purged after 90 days.

Support

Sayers provides support for Cloud and Firewall Lifecycle Services customers. Cloud customers receive first-call support as required in the Microsoft Partner agreement to address basic issues that can be resolved without escalation to Microsoft support. Firewall Lifecycle Services customers are provided support for firewalls included in their service agreements. Sayers does not provide other support beyond what is identified in SOWs. Issues with service delivery are addressed during client check-in calls and are documented as part of the project.

Principal Service Commitments and System Requirements

Regulatory Commitments

The organization complies with financial regulatory requirements; data is only retained when it is necessary to effectively conduct business activities, fulfill the mission, and comply with applicable laws and regulations including but not limited to:

- Providing an ongoing service or project
- Compliance with laws and regulations associated with financial and programmatic reporting by Sayers to funding agencies
- Security incidents and investigations
- Intellectual property preservation
- Litigation

Sayers undergoes both financial audits and annual SOC 2 audits.

Contractual Commitments

Sayers executes contractual agreements with its customers that outline its commitments related to the scope of work, security, confidentiality, availability, and other relevant service agreements. SOWs, MSAs, and non-disclosure agreements (NDAs) are maintained with customers depending on the services contracted for with Sayers.

System Design

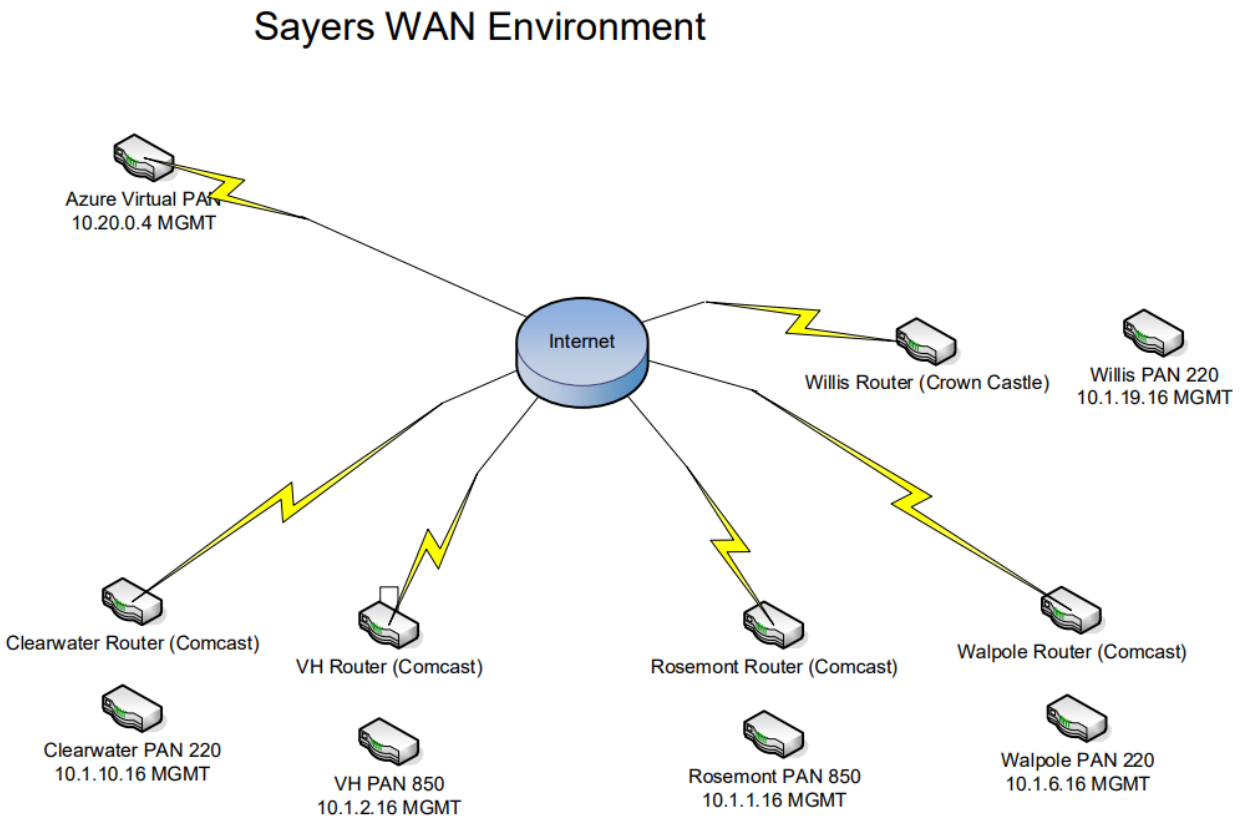
Sayers designs its personalized hardware and software services system to meet its regulatory and contractual commitments. These commitments are based on the services that Sayers provides to its clients, the laws and regulations that govern the provision of those services, and the financial, operational, and compliance requirements that Sayers has established for its services. Sayers establishes operational requirements in its system design that support the achievement of its regulatory and contractual commitments. These requirements are communicated in Sayers' system policies and procedures, system design documentation, and contracts with clients.

Components of the System Used to Provide the Services

Infrastructure

Sayers segregates its network with two wireless local area networks (WLANs), the Sayers Guest and Sayers Technology wireless networks. The Guest WLAN uses a captive portal to authenticate visitors, and the Sayers Technology WLAN uses enterprise security levels to authenticate users and devices. Both WLANs use 2.4GHz and 5GHz transmission rates with ARP filtering to prevent gateway spoofing attacks. The Technology WLAN's Service Set Identifier (SSID) is tied to the corporate Entra ID instance, while the Sayers Guest WLAN is set to the captive portal.

The following network diagram demonstrates the wide area network (WAN) environment and the virtual private network (VPN) connectivity between the organization's physical locations and Azure.



Software

The organization maintains a software inventory that lists the software used to provides its services, as well as the approved applications for end users. The software

inventory includes a description, application version, vendor, distributor, and other relevant information. Critical software in use by Sayers includes:

- Rapid7
- Tableau Server
- Zoom
- Ubistor
- Citrix ShareFiles
- M-Files Client
- Adobe Acrobat Pro
- Absolute VPN
- MS Teams
- Crystal Reports
- AvaTax
- eConnect for GP 2015
- ConnectWise Designer
- Smartsheet Data Connector
- Wasp Bar Code FontWare
- Maximum Data
- Clippership
- FedEx Ship Manager Server
- MS Power BI
- Jitterbit Cloud Data Loader
- DBAmp
- Tableau Desktop Pro
- HPI Smart EDI server
- WordPress
- DL Windows

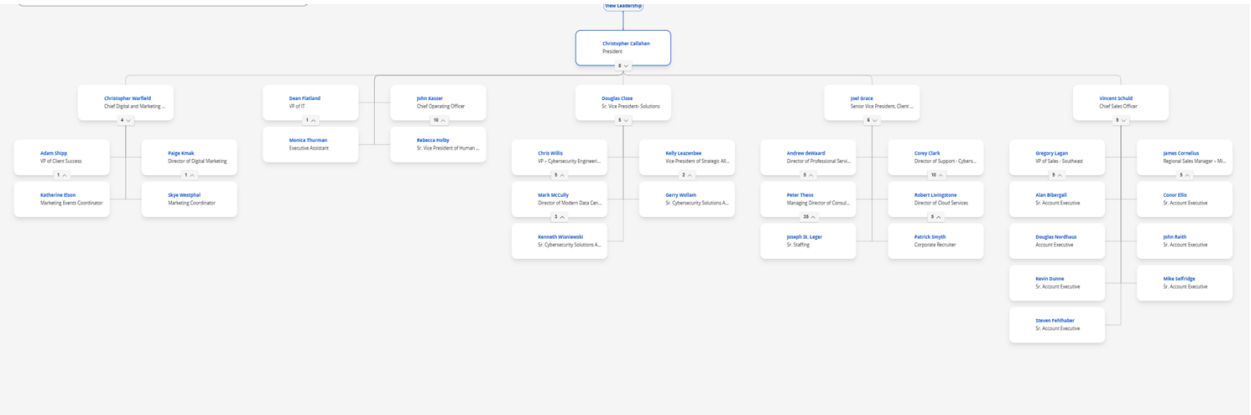
People

Sayers is overseen by an independent board of directors comprised of one independent member serving as the chairman, two Sayers representatives, and two members representing outside investors. The board meets in person on a quarterly basis to discuss company strategy, operations, and financials.

The organization maintains a traditional hierarchical structure with defined leadership, departments, and reporting lines. Direct reports to the Chief Executive Officer (CEO) and President include the Chief Digital and Marketing Officer, the VP of IT, the COO, the Senior VP of Solutions, the Senior VP of Client Services, and the Chief Sales Officer. A Senior Leadership team is composed of the CEO and President as well as all Vice President (VP) roles within the organization, and the following departments are maintained:

- Pre-sales and Sales Architects
- Services
- Marketing
- Sales
- Operations, Legal, and Project Management
- IT
- People

An organization chart, pictured below, is maintained to depict Sayers' hierarchical structure and management.



Data

Sayers maintains procedures for managing data securely. Data used to provide its services to clients is classified into the following categories: public, operational, and confidential. Guidance for the storage, transmission, consumption, and destruction of data in each category is provided within a Data Classification & Confidential Data Policy. Sayers also retains data as needed to conduct business and maintain compliance with applicable laws and regulations. Data is only retained when it is necessary to effectively conduct business activities, fulfill the organization's mission, and comply with regulatory requirements.

Data is protected both at rest and in transit using appropriate cryptographic algorithms. For data at rest, workstation drives are encrypted using BitLocker for Windows and File Vault for Macs. Full device encryption is required for Bring Your Own Device (BYOD) devices. Encryption is enforced using Intune policy settings. All servers are hosted in Azure as VMs and use default server-side encryption with Azure managed keys. For data in transit, site to site virtual private networks (VPNs) are established through the Palo Alto firewalls at each site. Sayers uses a hub-and-spoke model, where every office is a spoke that connects to the Azure hub. Sayers offices can only communicate with Azure; they are not configured to pass traffic directly to another site or via Azure. Laptops use the Absolute VPN client that encrypts traffic via a symmetric AES-256 bit key. Logon sessions to Entra ID, Palo Alto firewall consoles, network switch consoles, and tools such as Sentinel One are secured with HTTPS or Transport Layer Security (TLS) 1.2.

The SaaS tool Keeper is used to store internal IT secrets and secrets provided by customers, such as usernames and passwords. Login to Keeper occurs using Entra ID single sign on (SSO), and access to secrets is logged.

Processes and Procedures

Management has developed and communicated procedures to guide the provision of the organization’s services. Changes to procedures are performed annually and authorized by management. These procedures cover the following key security life cycle areas:

- Data classification
- Categorization of information

- Assessment of the business impact resulting from proposed security approaches
- Selection, documentation, and implementation of security controls
- Performance of annual management self-assessments to assess security controls
- Authorization, changes to, and termination of information system access
- Monitoring security controls
- Management of access and roles
- Maintenance and support of the security system and necessary backup and offline storage
- Incident response
- Maintenance of restricted access to system configurations, user functionality, master passwords, powerful utilities, and security devices

Relevant Aspects of the Control Environment, Risk Assessment Process, Information and Communication, and Monitoring

The security, availability, and confidentiality categories and applicable trust services criteria were used to evaluate the suitability of design and operating effectiveness of controls stated in the description. Security, availability, and confidentiality criteria and controls designed, implemented, and operated to meet them ensure that the system is protected against unauthorized access (both physical and logical). The controls supporting the applicable trust services security, availability, and confidentiality criteria are included in section IV of this report. Although the applicable trust services criteria and related controls are included in section IV, they are an integral part of Sayers' description of its personalized hardware and software services system.

Control Environment

Management Philosophy

Sayers management communicates its philosophy to all employees using an Employee Manual and Code of Business Conduct. The Employee Manual is provided to all employees during onboarding and must be acknowledged upon hire and upon any changes. The Code of Conduct, Integrity, and Ethics information is included within the Employee Manual and outlines Sayers' expectations for employee ethics and behavior.

Management philosophy is reinforced to employees through regular communication within the organization. One-on-one meetings are held between employees and their supervisors at the discretion of the supervisor. The Senior Leadership team, which is comprised of the CEO and President and all VP roles within the organization, have one-on-one meetings with each member on a weekly basis, as well as biweekly meetings with the team. Minimal separation is maintained between staff members and the CEO, which accelerates communications both up and down the organization's internal hierarchical structure.

Progressive discipline procedures up to and including termination are maintained and followed in instances of employee noncompliance.

Security, Availability, and Confidentiality Management

The organization's security, availability, and confidentiality requirements are managed using a combination of documented policies and procedures, management oversight, and network systems and hardware. These management practices are implemented in all areas of the control environment to protect systems, data, and personnel and to ensure compliance with industry best practices and standards.

Security, Availability, and Confidentiality Policies

Sayers develops and maintains policies that outline expectations and procedures for all employees. The creation of new policies is based on needs identified by the IT Subcommittee or Committee. Individuals with experience or responsibilities for data

or processes impacted by the policy are selected to draft new policies, which are reviewed by the Project Management team before presentation to and review by the IT Subcommittee. Existing policies are reviewed and updated as needed by the IT Subcommittee and approved by the IT Committee. A policy matrix is maintained to track policy information for each company policy document, including:

- Policy name
- Document type
- Category
- Policy owner
- Review cadence
- Date of last review
- Target deadline of next review
- Date of last revision
- Date of last approval
- Document location
- Notes

Company policies are maintained in a repository for employee reference. Policies must be acknowledged by all employees using AirMason on an annual basis, including:

- AI Policy
- Data Classification and Confidential Data Policy
- Device Management Policy
- Data Retention Policy
- Password Policy

Human Resources

Sayers maintains personnel security by defining procedures for the hiring and onboarding of its employees. When a manager is looking for an open role, a job description is created. Job descriptions are maintained for critical roles within the organization and outline include a brief overview of the organization, key responsibilities for each role, qualifications sought for the role, and a description of the ideal candidate for the role. Once a job description has been created, the organization's recruiter posts the job opening on the Sayers website, as well as on websites such as LinkedIn and Indeed. As candidates respond to the job opening and apply for the position, the recruiter narrows down a list of candidates by conducting phone screenings. The organization's Hiring Manager then conducts interviews with candidates. Additional interviews are held with additional personnel, and for technical roles, technical interviews are held. Final interviews are conducted with an executive, and candidates selected for hire are sent offer letters.

Upon signing and returning the offer letter, candidates undergo background checks. Background checks are comprehensive and include Social Security number (SSN) verification, former address checks, criminal history checks, drug screenings, and additional testing as required. Employment is contingent upon the results of the background check.

New hires complete onboarding within Paylocity, which includes providing basic information, setting up direct deposit, completing tax forms, and acknowledging company policies such as the Employee Manual and the Information Security Policy. IT sets up employee accounts and provisions access. Equipment is then sent to the new employee, and login credentials are provided on the first day of employment.

All employees must complete security awareness training upon hire and quarterly thereafter. Training is completed via Mimecast, and employees are required to complete training within two weeks of enrollment. Training topics include password management, secure data handling, phishing, and remote working.

Performance evaluations are conducted with all employees and their managers using TrackStar. Employees complete self-assessments, managers complete assessments, anonymous feedback is provided by other employees, and meetings are held to discuss the results of the evaluation.

Sayers also maintains and follows defined procedures for employee termination and offboarding. Exit interviews are held for voluntary terminations. HR notifies IT of the employee and the date of termination, and access is revoked. Equipment is also retrieved from the employee. Steps for employee termination and offboarding are tracked in Smartsheet.

Physical Security and Environmental Controls

Sayers maintains and enforces defined procedures to ensure the security of its six physical office locations:

- Vernon Hills, IL: Operations, Accounting, Accounts Payable, Warehouse, Configuration Space, HR, Sales, and Engineering
- Chicago, IL: Hoteling Space, Sales, Engineering
- Walpole, MA: Warehouse, Configuration Space, Sales, Engineering
- Clearwater, FL: Operations, Accounting, Accounts Receivable, Collections
- Rosemont, IL: Executives, Accounting, HR, Sales, Engineering
- Atlanta, GA: Hoteling Space, Sales, and Engineering

Access control systems are implemented within offices to restrict access to only authorized personnel. The Rosemont and Vernon Hills offices are locked at all times and are managed by ACS Trilogy access control, which is hosted on an Azure server VM. The Chicago suite is locked at all times and managed by an S2 Netbox access control system. The Walpole and Clearwater offices use hard keys. Access control badges are provided to new hires working from or visiting offices. Access is requested from the Senior VP of HR and is configured in the appropriate access control system by the Senior Application Developer and the VP of IT. Employees are only provisioned access to doors appropriate to their role and for hours appropriate to office working hours. Physical access is revoked upon termination.

The Walpole, Vernon Hills, and Rosemont offices are equipped with intrusion alarm systems, motion sensors, door contacts, and glass break sensors to monitor for and alert on authorized access to facilities. All employees have individual codes that are created upon hire by the monitoring vendor and disabled upon termination. When alarms are triggered, phone call notifications go to the VP of IT and the Office Manager.

Additionally, video surveillance systems are implemented within the Vernon Hills and Walpole offices. Cameras are in place to provide coverage of entrances and exits, and recording is based on motion. Video is stored locally on camera SD cards and is uploaded to cloud-based storage for 30 days. Full access to surveillance footage is limited to the VP of IT. The Chicago, Clearwater, and Rosemont offices are monitored using building surveillance systems.

Networking closets within Sayers office locations are appropriately secured. The Vernon Hills and Walpole offices' networking closets are secured using a lock and PIN.

Network closets at the Chicago, Clearwater, and Rosemont offices are secured with a lock and hard key.

Procedures for the identification and documentation of visitors to office facilities are maintained and enforced. The Chicago office relies on building management's visitor management system; the Vernon Hills, Walpole, Clearwater, and Rosemont offices allow visitors to knock on office suite doors for access, and paper visitor logs are used to capture each visitor's name, company, person visiting, and date and time in and out.

Sayers additionally maintains environmental security controls through fire detection and suppression systems supplied by building management. Fire detection and alarm systems with smoke detectors, strobes, and sirens, as well as annually inspected fire extinguishers, are provided by building management and present within the following Sayers offices:

- Vernon Hills, IL
- Chicago, IL
- Walpole, MA
- Clearwater, FL
- Rosemont, IL

Configuration Management

Sayers maintains defined standards for the configuration of systems. Steps involved in the hardening of systems include installing OS from a trusted source; installing patches and updates; removing vulnerable removing vulnerable software, services, and functionality; and installing local firewalls, antivirus, file permissions, logging, Active Directory group policy settings, and Rapid7 and SentinelOne agents. Windows and Mac endpoint configurations are managed using Intune, and servers adhere to the National Institute of Standards and Technology (NIST) 800-53 Section 5.3 configuration requirements. Changes to configurations are formally reviewed, approved, and documented using Sayers change management procedures.

Change Management

A formal change management process is used to facilitate changes within the organization. Changes are driven by change requests, which must be submitted and document the importance, urgency, and impact of changes; date of submission and date of change implementation; change owner; nature of the change; rollback plan; approver; implementor; and final result of the change (success or failure). All change requests are documented and tracked using a spreadsheet.

Change requests are reviewed by the IT Subcommittee to determine if the change has a significant impact. Changes with significant impacts must be scheduled. Complex changes are tested to determine the impact on usability and security. All changes require approval from the VP of it, the IT Subcommittee, or the IT Committee.

Network Monitoring

Sayers network monitoring occurs primary via automated systems and tools. Rapid7 InsightIDR ingests logs from multiple sources including Azure, Microsoft 365, Palo Alto

firewalls, and Rapid7 agents installed on all systems. Alerts are sent to the VP of IT and the Senior Application Developer to investigate. Logs are reviewed quarterly at a minimum, or once a month based on categorization.

Vulnerability Management

Sayers manages vulnerabilities to its environment through the use of designated tools and remediates vulnerabilities accordingly. Vulnerability scans are conducted on a routine basis using Rapid7 and include vulnerabilities by severity, severity trends, and risk score. Findings are reviewed by the IT Subcommittee, which prioritizes them for remediation and creates change requests for implementation. External vulnerabilities are identified through the use of BitSight and Security Scorecard to assess Sayers' public exposure. These reports are also reviewed by the IT Subcommittee. Rapid7 agents are installed via Group Policy on servers and via Intune for workstations. Additionally, each Palo Alto firewall is licensed with security services that block malicious files and block intrusion attempts. Palo Alto logs are ingested by Rapid7 for additional analysis and alerting.

Sayers also requires the use of up-to-date antivirus and anti-malware software on all company endpoints. Sayers primarily uses SentinelOne as an antivirus platform, with some systems remaining on the legacy Cylance Aurora platform. Endpoint agents are installed on all servers and workstations and are configured for automatic updating and tamper protection. Settings deployed to systems allow the agents to detect and protect systems with centralized alerting and logging. Agents are installed upon enrollment in Intune.

Vulnerabilities are additionally managed through regular system patching by Sayers. Patches are installed on a routine basis on all systems, including Azure workstation VMs, Windows workstations, and MacOS workstations.

Incident Response

Sayers prepares for incidents by ensuring employees complete Security Awareness Training that includes guidance on reporting potential incidents to IT. Reported or detected events are investigated to determine if they are false positives or if they rise to the level of an incident that requires activation of the Incident Response Plan. In the event of an actual incident, the IT Committee, which serves as the Incident Response team, is notified and the incident is entered on the IT Incident Response Tracker spreadsheet. All activity pertaining to the incident, including responses and timelines, is recorded. The Incident Response team reviews the ongoing incident and determines the best course to contain or eliminate the impact of the incident on operations, followed by recovery efforts. Post-incident, the team meets to review the team’s responses to the incident in order to identify opportunities for improvement.

The Incident Response Plan is tested at least annually through a tabletop exercise. Specific incident scenarios are used and discussed by the team. The results of the test and suggestions for improvement are included in the final incident report.

The Incident Response Plan is reviewed annually and updated as needed by the IT Subcommittee and is approved by the IT Committee.

Backup and Restoration

Sayers completes regular backups of systems and data. Sayers servers are hosted on Azure virtual machines (VMs), which are backed up and stored by Azure backup, with backup sets stored in a recovery vault. Daily backups are retained for 14 days, weekly backups are retained for 12 weeks, and monthly backups are retained for 60 months. Individual backup jobs are created for each backed up server. Recovery vaults use default Azure-managed encryption. Emailed backup alerts are monitored by the VP of IT and the Senior Application Developer for failures; in the event of a failure, Sayers IT investigates and re-runs the backup. Test restores are conducted annually to validate backups.

Business Continuity and Disaster Recovery

Sayers maintains defined procedures to ensure the continuation of business processes and recovery of critical systems in the event of a disaster or loss. While Sayers maintains six offices, there are no operational dependencies on any of them; offices are spaces for teams to collaborate, but all employees are capable of working remotely and/or from an alternate Sayers office. Internal IT systems are supported by Azure-hosted services and server VMs, and customer-facing Backbox services are hosted from leased space in a data center.

A Business Continuity Plan is maintained that identifies teams responsible for execution of the plan, teams who provide support for the plan, and priorities to observe during a disruptive incident. The teams' highest priority is safety of all Sayers staff, followed by establishing internal communications to determine the extent of the disruption and resources needed to restore normal functionality. Critical systems are identified with the tolerable outage duration and tolerable data loss point for each. Step-by-step guidance is provided to the Business Continuity team that identifies the person responsible, when the action should be carried out, and details on what to do. Similar guidance is provided for the Business Recovery Process to establish an alternate location and resources to restore normal functionality.

The Business Continuity Plan is reviewed annually by the IT Subcommittee and approved by the IT Committee. Tabletop exercises are used to test the plan and provide the Business Continuity and Disaster Recovery teams with a disruptive event and the resulting impact on Sayers operations, with a focus on five specific potential scenarios. The ability to recover from an Azure-related incident is validated through backup restoration testing.

Logical Access

Sayers has implemented logical access control systems to manage access to resources. Sayers relies on Active Directory and Entra ID for authentication and authorization. Two Azure-based domain controllers authenticate logins for network-connected systems and synchronize with Entra. Entra ID Conditional Access rules enforce MFA for all normal users, privileged users and for Absolute VPN connections. Role-based security groups have been created to provide access to employees based on their position.

Access is requested and authorized for new employees via an email to the Senior VP of HR. These access requests are picked up by the VP of IT or the Senior Application

Developer for implementation. Requests to disable access for terminated employees follow the same process.

Sayers maintains account credential policies, including policies over the construction of secure passwords. Passwords for new users are provided by Dean Flatland (VP of IT) during onboarding and expire upon 1st login. Passwords must consist of at least eight characters and expire every 180 days. Active Directory password complexity requirements are enabled, and the last five passwords cannot be re-used. In the event a password is forgotten or is expired, employees can use the Microsoft Self Service Password Reset (SSPR) to reset their passwords. Users must have provided answers for security questions during onboarding; the answers to security questions and their MFA device are used to validate their identity.

User account reviews are conducted twice a year informally; the VP of IT reviews active user accounts to identify any terminated employees who are still active and additionally spot checks user permissions.

Vendor Management

Sayers manages the vendors it engages with to provides its services to ensure that vendors meet the organization's standards for security and compliance. Sayers requires new vendor engagements to be requested, and new vendors are vetted. Requests to engage with new vendors are discussed during IT Subcommittee meetings, where members review the vendor, services provided, and the criticality of the vendor. In initial vendor review and due diligence, compliance audit reports are reviewed when provided. Vendors are tracked using Smartsheet and the following is tracked for all vendors:

- Vendor name
- Service provided
- Access to financial/confidential information
- NDA in place
- Contract in place
- Service provider's and Sayers' responsibilities
- Completion of onboarding risk assessment
- URL to compliance trust center
- Target review date
- Date of last review
- Notes

Sayers also completes annual reviews of third-party vendors to ensure their continued compliance and security. Annual vendor reviews involve obtaining and reviewing the most recent compliance audit reports.

Risk Assessment Process

Sayers maintains procedures for the routine identification, assessment, and management of risks to the organization. An assessment of potential risks and vulnerabilities serves as the basis for compliance efforts. The VP of IT is responsible for overseeing the process of risk management and maintains asset inventories for the organization. Threats to confidentiality, integrity, and/or availability are considered for each asset, which facilitates the identification of risks. Additionally, vulnerabilities in information systems are identified and documented.

The Sayers risk management process is ad-hoc; risk is discussed at all IT Subcommittee meetings. When the subcommittee identifies new risks, they are added to a risk register. Risks are discussed and rated by impact and likelihood to determine a risk rating. Risks are rated by probability and criticality and receive the following ratings: Very Low, Low, Moderate, High, and Critical. Existing controls to reduce risk are also identified, and additional necessary controls are planned.

The full risk register is reviewed by the IT Committee on an annual basis. If significant changes lead to the introduction of new risks, changes to the risk register are reviewed and approved by the IT Committee. The risk register tracks the following for each identified risk:

- Risk category
- Name
- Impacted asset
- Threat and description
- Likelihood, impact, and risk level
- Current controls
- Percent mitigated
- Remaining risk
- Risk treatment details

Information and Communication Systems

Sayers maintains an information security program supported by a comprehensive information security policy. The Information Security Policy is intended to define technical controls and security configurations for users and IT administrators used to ensure integrity and availability of data, including policies and guidance concerning acceptable use of technology resources. The policy applies to the Sayers network system and all users. The policy addresses topics including but not limited to:

- Employee requirements and expectations
- Prohibited activities
- Reporting security incidents and incident management
- Confidential information handling
- Access control and user account termination
- Confidentiality agreement
- Passwords
- Identification and authentication requirements
- Firewalls and permanent connections
- Anti-malware
- Encryption and key management
- Physical security
- Telecommuting
- Data and media disposal
- Bring Your Own Device (BYOD) devices
- Audit controls
- Data integrity
- Security Awareness Training

The IT Committee receives information from the IT Subcommittee to make decisions regarding major changes or implementations to the information security program and policies. The committee meets monthly to discuss security issues and IT projects, to go over concerns from the previous month, and to review items passed up from the subcommittee.

Monitoring Controls

Sayers monitors operational quality and control within the organization using key performance indicators (KPIs) from various tools. The following KPIs are analyzed to measure performance and ensure quality in service delivery:

- Revenue by year GP by year, GP by practice, revenue by month, segmented by geographical location, segmented by sec/data center/services
- Top accounts
- Close won over $5,000
- Close by representative
- Pipeline by storage
- GP by partner
- Revenue by partner
- GP by representative
- Pipeline for the quarter

Additionally, Clari allows the organization to perform Salesforce data inspection and revenue reporting on pipeline opportunities, trends, and forecasting.

Employee performance is measured and monitored through performance evaluations. Evaluations are conducted with all employees and their managers using TrackStar.

Changes to the System During the Period

There were no changes that are likely to affect report users' understanding of the personalized hardware and software services system during the period from August 1, 2024, through July 31, 2025.

Complementary User-Entity Controls

Sayers' services are designed with the assumption that certain controls are implemented by user organizations. In certain situations, the application of specific controls at the user organization is necessary to achieve control objectives included in this report. Sayers' management makes control recommendations to user organizations and provides the means to implement these controls in many instances. Sayers also provides best practice guidance to clients regarding control elements outside the sphere of Sayers responsibility.

This section describes additional controls that should be in operation at user organizations to complement the Sayers controls. Client Consideration recommendations include:

- User organizations should implement sound and consistent internal controls regarding general IT system access and system usage appropriateness for all internal user organization components associated with Sayers.

- User organizations should practice removal of user accounts for any users who have been terminated and were previously involved in any material functions or activities associated with Sayers' services.

- Transactions for user organizations relating to Sayers' services should be appropriately authorized, and transactions should be secure, timely, and complete.

- For user organizations sending data to Sayers, data should be protected by appropriate methods to ensure confidentiality, privacy, integrity, availability, and non-repudiation.

- User organizations should implement controls requiring additional approval procedures for critical transactions relating to Sayers' services.

- User organizations should report to Sayers in a timely manner any material changes to their overall control environment that may adversely affect services being performed by Sayers.

- User organizations are responsible for notifying Sayers in a timely manner of any changes to personnel directly involved with services performed by Sayers. These personnel may be involved in financial, technical, or ancillary administrative functions directly associated with services provided by Sayers.

- User organizations are responsible for adhering to the terms and conditions stated within their contracts with Sayers.

- User organizations are responsible for developing, and if necessary, implementing a business continuity and disaster recovery plan (BCDRP) that will aid in the continuation of services provided by Sayers.

The list of user organization control considerations presented above and those presented with certain specified control objectives do not represent a comprehensive set of all the controls that should be employed by user organizations. Other controls may be required at user organizations. Therefore, each client's system of internal controls must be evaluated in conjunction with the internal control structure described in this report.

Section IV:

Trust Services Categories, Criteria, Related Controls, and Tests of Controls

Applicable Trust Services Criteria Relevant to Security, Availability, and Confidentiality

Although the applicable trust services criteria and related controls are presented in section IV, "Trust Services Categories, Criteria, Related Controls, and Tests of Controls," they are an integral part of Sayers' system description throughout the period August 1, 2024, to July 31, 2025.

Security

The trust services criteria relevant to security address the need for information and systems to be 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 the service organization's ability to achieve its service commitments and system requirements.

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 achievement of Sayers' service commitments and system requirements. Controls over security prevent or detect the breakdown and circumvention of segregation of duties, system failure, incorrect processing, theft or other unauthorized removal of information or system resources, misuse of software, and improper access to or use of, alteration, destruction, or disclosure of information.

Availability

The trust services criteria relevant to availability address the need for information and systems to be available for operation and use to achieve the service organization's service commitments and system requirements.

Availability refers to the accessibility of information used by Sayers' systems, as well as the products or services provided to its customers. While the availability objective does not address system functionality (the specific functions a system performs) or usability (the ability of users to apply system functions to the performance of specific tasks or problems), it does address whether systems include controls to support accessibility for operation, monitoring, and maintenance.

Confidentiality

The trust services criteria relevant to confidentiality address the need for information designated as confidential to be protected to achieve the service organization's service commitments and system requirements.

Confidentiality addresses Sayers' ability to protect information designated as confidential from its collection or creation through its final disposition and removal from Sayers' control in accordance with management's objectives. Information is confidential if the custodian of the information is required to limit its access, use, and retention and restrict its disclosure to defined parties. Confidentiality requirements may be contained in laws or regulations or in contracts or agreements that contain commitments made to customers or others. The need for information to be confidential may arise for many different reasons.

Confidentiality is distinguished from privacy in that privacy applies only to personal information, whereas confidentiality applies to various types of sensitive information. In addition, the privacy objective addresses requirements regarding collection, use, retention, disclosure, and disposal of personal information. Confidential information may include personal information as well as other information, such as trade secrets and intellectual property.

Trust Services Criteria for the Security, Availability, and Confidentiality Categories

Control Environment

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC1.1	The entity demonstrates a commitment to integrity and ethical values.		
CC1.1.1	The organization maintains an employee handbook that must be acknowledged by all employees and reviews the handbook on an annual basis, with updates made as necessary.	Reviewed the Sayers Employee Manual (dated January 10, 2025) and verified that the manual includes all relevant policies and addresses topics including but not limited to: • Employment Classification • Resignation or separation • Benefits • Conduct and work rules • Code of Business Conduct • Progressive discipline • Working remotely • Access to personnel files • Non-disclosure • Merit reviews - 90-day new hire and annual performance reviews • Safety and security • Email, internet, and social media usage Interviewed the Senior Vice President (VP) of Human Resources (HR) and determined that an Employee Handbook is maintained and reviewed at least annually by the Senior VP of HR; updates are made as necessary, including updates proposed for consideration by AirMason, and the Chief Executive Officer (CEO) approves handbook updates Observed the revision date within the Sayers Employee Manual and verified that the manual was last reviewed and updated on January 10, 2025	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Observed handbook acknowledgments for a sample of employees hired during the audit period (4 of 42) and verified that the handbook is acknowledged in Paylocity during onboarding for all employees	
CC1.1.2	The organization defines standards for employee conduct through a Code of Business Conduct within the Employee Manual.	Reviewed the Sayers Employee Manual (dated January 10, 2025) and verified that the Code of Business Conduct outlines the following: Each employee is responsible for conducting themselves in a professional manner appropriate for a business setting while conducting company business/on company property; disciplinary actions may result, up to and including termination, for adverse actions and behavior Observed handbook acknowledgments for a sample of employees hired during the audit period (4 of 42) and verified that the handbook is acknowledged in Paylocity during onboarding for all employees	No Relevant Exceptions Noted
CC1.1.3	The organization maintains and follows a defined hiring process for new employees.	Interviewed the Senior VP of HR and determined that the organization follows a defined hiring process for new employees: • Job postings are made on the Sayers website and other sites like LinkedIn and Indeed • Phone screenings are held by the internal recruiter to narrow down candidates • Interviews with candidates are conducted by various individuals, including the Hiring Manager • Final interviews are conducted with executives • Offer letters are sent to selected candidates, which must be signed and returned • Background checks are completed on candidates following return of the offer letter	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• Onboarding is initiated Observed the new hire checklist and verified that the spreadsheet tracks steps for onboarding, including: • Employee name • Dates offer letter sent and received • Dates drug screening sent and received • Background check • Computer, extension, email, and badge requested • "Fully complete" checkbox when all tasks have been completed	
CC1.1.4	The organization facilitates new employee onboarding using a checklist tracked in Smartsheet.	Interviewed the Senior VP of HR and determined that a defined onboarding process is followed for new employees: • Onboarding is initiated in Paylocity • Equipment is shipped to the new hire • Login credentials are provided to the new hire • The new hire is registered in systems including Motivosity for team feedback, Kimble for expense reporting, and TrackStar for performance evaluations • Reviews are held with the employee following 90 days of employment • Onboarding steps are tracked in Smartsheet Observed onboarding files for a sample of employees hired during the audit period (4 of 42) and verified that files included the following: • Offer letters • Background check reports • Email requests to IT for user accounts • Paylocity policy acknowledgments including	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		the Employee Manual and the Information Security Policy	
CC1.1.5	The organization maintains defined termination and offboarding procedures for employee separation, which are tracked in Smartsheet.	Interviewed the VP of HR and determined that the following steps are completed for employee terminations: • Exit interviews are held for voluntary terminations • HR notifies IT of the date of termination • Equipment is returned to the organization • Confirmation of account termination is documented • Termination is tracked in Smartsheet Observed the termination checklist and verified that a spreadsheet is used to track the following: • Employee name • Email address • Position • Date of hire • Date of Termination • Terminated or resigned • Salary through last day of employment • Accrued and unused paid time off (PTO) Observed termination documentation for a sample of employees terminated during the audit period (3 of 21) and verified that the organization reviews credential validity, removes physical devices, and prevents the use of credentials that are no longer valid	No Relevant Exceptions Noted
CC1.2	The board of directors demonstrates independence from management and exercises oversight of the development and performance of internal control.		
CC1.2.1	The organization maintains an independent board of directors, which meets on a routine basis to discuss company strategy, operations, and financials.	Interviewed the Chief Operating Officer (COO), the Chief Executive Officer (CEO), the Chief Financial Officer (CFO), the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		that the Board of Directors is comprised of one independent member serving as the chairman, two Sayers representatives, and two members representing outside investors; the board meets in person on a quarterly basis Observed board meeting minutes for a sample of quarters during the audit period (3 of 4) and verified that all board members are present at meetings, and meeting notes document the following: • List of attendees • Call to order • Resolutions • Operations update • Strategic activities • Financials • Board approvals	
CC1.3	Management establishes, with board oversight, structures, reporting lines, and appropriate authorities and responsibilities in the pursuit of objectives.		
CC1.3.1	The organization maintains a traditional hierarchical structure with established departments and reporting lines.	Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that the organization is structured into a Senior Leadership team and the following departments: • Pre-sales and Sales Architects • Services • Marketing • Sales • Operations, Legal, and Project Management • IT • People Observed the organization chart and verified that the organization maintains a traditional hierarchical structure with the President at the top; direct reports to the President include the Chief Digital and Marketing Officer, the VP of IT, the COO, the Senior VP of Solutions, the Senior VP of Client	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Services, and the Chief Sales Officer	
CC1.4	The entity demonstrates a commitment to attract, develop, and retain competent individuals in alignment with objectives.		
CC1.4.1	The organization requires the completion of background checks on all new hires.	Reviewed the Sayers Background Check Policy (dated May 7, 2025) and verified that background checks include Social Security number (SSN) verification, former address checks, criminal history checks, drug screenings, and additional testing as required; employment is contingent upon the results of the background check Interviewed the Senior VP of HR and determined that background checks and drug screenings are conducted on all employees following return of the new hire's offer letter Observed background checks for a sample of employees hired during the audit period (4 of 42) and verified that checks include the following: • National criminal search • Sex offender search • SSN verification • County criminal search • Global sanctions search	No Relevant Exceptions Noted
CC1.5	The entity holds individuals accountable for their internal control responsibilities in the pursuit of objectives.		
CC1.5.1	The organization maintains and enforces progressive discipline procedures to address instances of employee noncompliance.	Interviewed the Senior VP of HR and determined that the organization follows progressive discipline procedures up to and including termination for employees that fail to comply with objectives; performance improvement plans (PIPs) may be included in written warnings	No Relevant Exceptions Noted
CC1.5.2	The organization completes annual performance evaluations with all employees and their managers.	Interviewed the Senior VP of HR and determined that performance evaluations are conducted; employees complete self-assessments, the employee's manager completes an	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		assessment, and a meeting is held to discuss the reviews Observed the use of TrackStar for performance evaluations and verified that employees are scored on different topics from one to five; performance evaluations may include anonymous feedback from other employees, comments from the employee, and comments from the manager Observed performance evaluations for a sample of existing employees during the audit period (17 of 169) and verified that annual performance evaluations are completed and documented	
CC1.5.3	The organization monitors operational quality and control in routine meetings using key performance indicators (KPIs).	Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that operational quality and control issues are discussed in weekly meetings with the Director of Operations and Finance; additionally, internal sync calls and monthly meetings on the organization's largest clients are held to ensure quality control and identify opportunities for improvement Observed Salesforce KPIs and verified that the following KPIs are monitored to measure performance and ensure operational quality and control: • Revenue by year GP by year, GP by practice, revenue by month, segmented by geographical location, segmented by sec/data center/services • Top accounts • Close won over $5,000 • Close by representative • Pipeline by storage • GP by partner • Revenue by partner	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• GP by representative • Pipeline for the quarter Observed Clari and verified that various views allow the organization to perform Salesforce data inspection and revenue reporting on pipeline opportunities, trends, and forecasting	

Communication and Information

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC2.1	The entity obtains or generates and uses relevant, quality information to support the functioning of internal control.		
CC2.1.1	The organization classifies the data used to provide its services to clients and handles data according to its classification.	Reviewed the Sayers Data Classification & Confidential Data Policy (dated November 6, 2024) and verified the following: • Data classification levels include Public, Operational, and Confidential • Guidance for the storage, transmission, consumption, and destruction of each level of classification is defined • Handling and security controls for confidential data include clean desk policies, encryption, network segmentation, physical security, and transmission via email, paper, or fax Observed Absolute Virtual Private Network (VPN) client encryption settings and verified that AES 256 is enabled for secure access to Sayers networks	No Relevant Exceptions Noted
CC2.2	The entity internally communicates information, including objectives and responsibilities for internal control, necessary to support the functioning of internal control.		
CC2.2.1	The organization maintains formal documented job descriptions that outline responsibilities for roles within the organization.	Interviewed the Senior VP of HR and determined that job descriptions are maintained for critical roles; job descriptions are reviewed and revised as necessary when a new job posting is made Observed examples of job descriptions for a variety of roles within the organization and verified that the organization communicates the responsibilities for each role; all job descriptions include a brief overview of the organization, key responsibilities for each role, qualifications sought for the role, and a description of the ideal candidate for the role	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Observed the maintenance of job descriptions and verified that job descriptions are maintained by HR for critical roles, including but not limited to: • Senior Network WAN Engineer • Sales Support Administrator • Partner Alliances Coordinator • Program Manager • Senior Security Implementation Engineer • Senior Business Continuity Architect	
CC2.2.2	The organization requires all employees to undergo security awareness training at hire and quarterly thereafter.	Reviewed the Information Security Policy (dated October 24, 2024) and verified the following: • Training is the responsibility of the VP of IT • Documentation of training is maintained • Training is provided to all new workforce members and to all employees on a quarterly basis • Security reminders are sent on a regular basis to address password security, malicious software, incident identification and response, and access control Interviewed the Senior VP of HR and determined that employee security awareness training is provided quarterly via Mimecast, and employees are required to complete training within two weeks of enrollment; training topics include password management, secure data handling, phishing, and remote working Observed an example of training materials for data security and categorization and verified that topics addressed include the following: • The importance of data security	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• Common threats and challenges • Best practices • Data loss prevention • Sensitivity label definitions Observed a Microsoft Teams message "FBI Smishing Text Warning" shared by the Senior VP of Solutions (dated March 13, 2025) and verified that the organization alerts employees of smishing threats Observed a Microsoft Teams message "Excellent Cyber Survival Website for Everyday People" (dated May 21, 2025) and verified that the organization alerts employees to cybersecurity training resources and best practice materials Observed training completion for a sample of employees hired during the audit period (4 of 42) and verified that each completed new hire security awareness training within 30 days of hire Observed training completion for a sample of existing employees during the audit period (17 of 169) and verified that all employees completed security awareness training and data security training	
CC2.2.3	The organization maintains a policy repository for employee reference and requires annual policy acknowledgments by employees.	Interviewed the Senior VP of HR and determined that AirMason is used to store company policies for reference, and annual policy acknowledgments are required using AirMason Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that changes to policies are initiated by the IT Subcommittee/Committee	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Observed AirMason and verified that internal policies are stored, including the AI Policy, the Data Classification and Confidential Data Policy, the Device Management Policy, the Data Retention Policy, and the Password Policy; AirMason is used for the storage, delivery, and acknowledgment of internal policies for all employees Observed policy acknowledgments for a sample of existing employees during the audit period (17 of 169) and verified that employees acknowledged the Information Security Policy, the AI Policy, the Data Classification and Confidential Data Policy, the Device Management Policy, the Data Retention Policy, and the Password Policy Observed Paylocity and verified that Paylocity is used for the storage, delivery, and acknowledgment of the Information Security Policy, the Employee Manual, and internal policies for new hires	
CC2.2.4	The organization holds regular meetings with senior leadership and annual meetings with all employees to communicate regarding business updates and company operations.	Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that the Senior Leadership team is comprised by the Senior VP of HR, the VP of IT, the Senior VP of Client Services, the Senior VP of Solutions, the CFO, the COO, and the Chief Sales Officer; the team meets periodically to provide status updates on areas of the business and discuss anything pertinent to the company Observed the all-company meeting presentation and verified that the meeting includes updates from department leaders on accomplishments from the prior	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		year, events, and targets and goals for the following year Observed calendar entries for a sample of Senior Leadership team meetings during the audit period (3 of 12) and verified that meetings occur on a defined cadence	
CC2.3	The entity communicates with external parties regarding matters affecting the functioning of internal control.		
CC2.3.1	The organization maintains lines of communication with external users for support needs.	Observed the Sayers Contact Us page on the company website and verified that the following contacts are provided to external users: • General support toll-free phone number and email address • Azure and Microsoft 365 support toll-free phone number and email address • Citrix CSP support toll-free phone number Observed the use of Salesforce to track customer tickets and requests for support and verified that support requests are picked up by an available engineer, who calls the customer to follow up and identify the customer's support needs	No Relevant Exceptions Noted
CC2.3.2	The organization executes contracts with its clients that cover the scope of work, security, confidentiality, and other relevant service agreements.	Observed client contracts for a sample of Cloud – Professional Services clients (3 of 9), Cybersecurity – Professional Services clients (3 of 27), Cybersecurity - Sayers Lifecycle Services/Proactive Services clients (3 of 10), and Infrastructure - Professional Services clients (3 of 17) and verified that Statements of Work (SOWs), Master Services Agreements (MSAs), and non-disclosure agreements (NDAs) are maintained with customers depending on the services contracted for with Sayers Observed examples of SOWs and verified that they follow a	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		standardized format and include the following: • Document control table - version, version date, nature of change • Executive summary • Requirement (client problem to solve) • Governance - kickoff meeting agenda • Services - phased design, discovery, planning, and implementation steps • Deliverables - services, deliverable/documentation, and acceptance criteria • Prerequisites, assumptions, and scope exclusions • Project staffing - Sayers and client responsibilities • Cancellation • Project fees and payment • Location, client contacts, and client invoicing contacts • Signature page • Change request form Observed examples of MSAs and verified that MSAs include information on performance, risk, non-disclosure, security, and other relevant service agreements	

Risk Assessment

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC3.1	The entity specifies objectives with sufficient clarity to enable the identification and assessment of risks relating to objectives.		
CC3.1.1	The organization maintains inventories of its assets to facilitate the performance of an organizational and technical risk assessment.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that the VP of IT is responsible for the risk assessment process and maintains a system inventory; threats to confidentiality, integrity, and/or availability are considered for each asset Observed the inventory of assets throughout the organization's environment and verified that the organization manages assets to facilitate the performance of an organizational and technical risk assessment; the inventories include the adequate details pertaining to the assets and peripherals present within the organization's networks, facilitating the identification of vulnerabilities that may affect said assets Observed the Sayers Software List and verified that the organization maintains an inventory export from InTune that identifies the following for each approved software application in use: application name, description, version, vendor, and OS	No Relevant Exceptions Noted
CC3.2	The entity identifies risks to the achievement of its objectives across the entity and analyzes risks as a basis for determining how the risks should be managed.		
CC3.2.1	The organization continually identifies, assesses, and manages risks to the company and tracks all risks in a risk register.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified the following: • An assessment of potential risks and vulnerabilities serves as the basis for compliance efforts • Security risks are reassessed, and security measures and safeguards are evaluated for effectiveness	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• The VP of IT is responsible for the risk assessment process • Vulnerabilities in information systems are identified and documented • Risks are rated by probability and criticality: Very Low, Low, Moderate, High, and Critical • Security measures to address risks are identified with timeline, costs, and ownership Interviewed the VP of IT, the Senior VP of Solutions, and the VP of Project Management and determined the following: • The risk management process is ad-hoc, and risks are discussed at all IT Subcommittee meetings • When new risks are identified, they are added to the risk register • Existing controls to reduce risk are discussed, and additional controls are planned Observed the risk register and treatment plan and verified the following: • Scope is defined as all Sayers sites and departments, as well as IT systems and services • Criteria defines threats and risks to be considered • Methodology steps are enumerated • The register tracks each risk-by-risk category, name, impacted asset, threat and description, likelihood and impact, current controls, percent mitigated, remaining risk, and risk treatment details • Risk categories include Existential, External, Operational, Personnel, and Technological	

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• Asset categories include Brand, End User Devices, People, Servers, Supply Chain, and Technology	
CC3.3	The entity considers the potential for fraud in assessing risks to the achievement of objectives.		
CC3.3.1	The organization considers the risk of fraud during its risk assessment process.	Observed the risk register and treatment plan and verified that risk of fraud is considered through the risk of data loss or theft, insider disclosure of protected data, and insider data modification	No Relevant Exceptions Noted
CC3.4	The entity identifies and assesses changes that could significantly impact the system of internal control.		
CC3.4.1	The organization considers significant changes and resulting risks during its risk assessment process.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified the following: • An assessment of potential risks and vulnerabilities serves as the basis for compliance efforts • Security risks are reassessed, and security measures and safeguards are evaluated for effectiveness • Vulnerabilities in information systems are identified and documented • Risks are rated by probability and criticality: Very Low, Low, Moderate, High, and Critical • Security measures to address risks are identified with timeline, costs, and ownership Interviewed the VP of IT, the Senior VP of Solutions, and the VP of Project Management and determined that the full risk register is reviewed by the IT Committee on an annual basis; if there are significant changes due to new risks, the changes are raised with the subcommittee to the committee for approval	No Relevant Exceptions Noted

Monitoring Activities

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC4.1	The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.		
CC4.1.1	The organization undergoes annual independent financial audits.	Observed the Sayers Technology Holdings, Inc. and Subsidiaries Audited Financial Statements (dated December 31, 2024) and verified that the Independent Auditor's Report and Consolidated Financial Statements state that financial statements present fairly, in all material respects, the financial position of Sayers Technology Holdings as of December 31, 2024	No Relevant Exceptions Noted
CC4.1.2	The organization undergoes annual internal and external audits of its security controls.	Observed assessments of the security controls in place at the organization and verified that the organization considers separate evaluations on a repetitive basis of its controls, and these evaluations are based on industry standards and best practices; they are also completed by independent third parties.	No Relevant Exceptions Noted
CC4.2	The entity evaluates and communicates internal control deficiencies in a timely manner to those parties responsible for taking corrective action, including senior management and the board of directors, as appropriate.		
CC4.2.1	The organization communicates on a defined basis with the Board of Directors regarding operational quality and control.	Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that quarterly presentations are made to the Board of Directors on results Observed board meeting minutes for a sample of quarters during the audit period (3 of 4) and verified that board meeting minutes include an operations update and financials review	No Relevant Exceptions Noted

Control Activities

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC5.1	The entity selects and develops control activities that contribute to the mitigation of risks to the achievement of objectives to acceptable levels.		
CC5.1.1	The organization identifies existing risk mitigation controls and develops new control activities to treat risk during its risk assessment process.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that security measures to address risks are identified with timeline, costs, and ownership Interviewed the VP of IT, the Senior VP of Solutions, and the VP of Project Management and determined that existing controls to reduce risk are discussed, and additional controls are planned Observed the risk register and treatment plan and verified that the register tracks percent of mitigation for risk, as well as risk treatment details	No Relevant Exceptions Noted
CC5.2	The entity also selects and develops general control activities over technology to support the achievement of objectives.		
CC5.2.1	The organization maintains control activities and procedures surrounding the use of AI.	Reviewed the Sayers AI Policy (dated May 12, 2025) and verified the following: • Microsoft Copilot is authorized for internal use, including web search, graphic art, content creation, content improvement, and content optimization • Exceptions for the use of other AI tools can be requested from the IT Committee provided they do not compromise Sayers' security and/or privacy • Confidential information is not to be shared with any AI tool without approval • Guidance for employee usage of Copilot includes respecting data privacy and confidentiality, respecting social and ethical values of Sayers, respecting human rights, and respecting the	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		quality and reliability of products and services Interviewed the COO, the CEO, the CFO, the VP of IT, the VP of Project Management, the Senior VP of Solutions, and the Senior VP of Client Services and determined that and AI committee exists within the organization to discuss and recommend action on the use of AI	
CC5.2.2	The organization maintains a comprehensive information security policy to define technical controls and security configurations for users and IT administrators used to ensure the integrity and availability of data.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that the policy is intended to define technical controls and security configurations for users and IT administrators used to ensure the integrity and availability of data, including policies and guidance concerning acceptable use of technology resources; topics addressed in the Information Security Policy include but are not limited to: • Employee requirements and expectations • Prohibited activities • Reporting security incidents and incident management • Confidential information handling • Access control and user account termination • Confidentiality agreement • Passwords • Identification and authentication requirements • Firewalls and permanent connections • Anti-malware • Encryption and key management • Physical security • Telecommuting • Data and media disposal • Bring Your Own Device (BYOD) devices • Audit controls • Data integrity	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		• Security Awareness Training Interviewed the VP of IT and determined that the Information Security Policy and related policies provide employees guidance on Sayers' expectations and their responsibilities related to information security	
CC5.3	The entity deploys control activities through policies that establish what is expected and in procedures that put policies into action.		
CC5.3.1	The organization maintains documented procedures for business continuity and disaster recovery and tests these procedures on a routine basis.	Reviewed the Business Continuity Plan (dated April 29, 2025) and verified that the organization has established policies and procedures to support contingency planning controls; the plan outlines the following: • In-scope locations, as well as responsibilities and priorities • Instances in which the plan would be triggered and procedures for continuity and recovery efforts • Business recovery processes and responsible parties • Processes and procedures for both administrative and technical incidents • Procedures for testing the plan Interviewed the VP of IT and the COO and determined that a business continuity plan is maintained that identifies teams responsible for execution of the plan, teams who provide support for the plan, an identifies priorities to observe in during a disruptive incident; step-by-step guidance is provided to the Business Continuity team that identifies the person responsible, when the action should be carried out, and details on what to do, and similar guidance is provided for the Business Recovery Process to establish an alternate location and resources to restore normal functionality	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Observed backup and restoration testing from during the audit period and verified that the organization tests the integrity and completeness of backups performed on its environments in support of its disaster recovery efforts; backups were performed and recovered without incident for both tests conducted during the audit period Observed notes and the calendar invite for business continuity testing conducted during the audit period and verified that the organization implements and practices business continuity procedures through testing	
CC5.3.2	The organization conducts data backups and backup restoration testing according to procedures defined in company policy.	Reviewed the Sayers Data Backup Policy (dated October 16, 2024) and verified that backup and backup retention schedules are defined Interviewed the VP of IT and determined the following: • Sayers servers are hosted on Azure virtual machines (VMs), which are backed up and stored by Azure Backup, with backup sets stored in a recovery vault • Backup retention is determined by frequency of backup • Individual backup jobs are created for each backed up server • Recovery vaults use Azure-managed encryption • Emailed backup alerts are monitored by the VP of IT and the Senior Application Developer for failures Observed backup settings and verified that the organization creates data backups based on data priorities and classifications; the backup settings are set to	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		perform recurring backups with retention periods that conform with data retention requirements, and backups are performed using the Azure backup utility Observed data backup test restore reports dated August 14, 2024, and May 12, 2025, for tests of file-level backups and VM backups and verified that reports track the date, objective, and results of the test; both tests were successful	
CC5.3.3	The organization tests its Incident Response Plan at least annually through tabletop exercises.	Reviewed the Sayers Incident Response Policy and verified it identifies the following: • The five phases of incident response, including prepare, detect, respond, recover, post-incident review • Contact table identifying the IT Committee as the IR Team with support from Operations & Communications and Information Technology team leads • The requirement for the incident response plan to be subject to an annual review and update as needed or upon significant infrastructure changes Interviewed the VP of IT and the VP of Project Management and determined that the Incident Response Plan is tested at least annually through a tabletop exercise; results of tests and suggestions for improvement are included in the final report Observed the Sayers Cybersecurity Incident Tabletop Exercise from during the audit period and verified that a tabletop exercise was conducted; documentation identifies attendees, simulated incident and impact, and observations from the Sayers team's response to the simulated incident	No Relevant Exceptions Noted

Logical and Physical Access Controls

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC6.1	The entity implements logical access security software, infrastructure, and architectures over protected information assets to protect them from security events to meet the entity's objectives.		
CC6.1.1	The organization securely manages encryption keys.	Reviewed the Sayers Encryption Policy (dated March 7, 2025) and verified the following: • Ciphers must meet or exceed AES-compatible or partially AES-compatible requirements according to NIST FIPS 140-2 • Key exchanges must use Diffie-Hellman, IKE, or ECDH, and endpoints must be authenticated prior to exchange of keys • Authentication servers must have a valid installed certificate from a known, trusted advisor • Keys must be securely generated and stored Interviewed the VP of IT and determined that the organization uses Keeper to store internal IT secrets and secrets provided by customers, such as usernames and passwords; login to Keeper occurs via Entra ID single sign on (SSO), and access to secrets is logged Observed a sample of Azure workstation VMs (5 of 67) and verified that server-side encryption with Azure managed keys was enabled Observed Keeper and verified that Keeper is used to store secrets and passwords for Sayers internal IT and for customer-provided information	No Relevant Exceptions Noted
CC6.1.2	The organization uses an access control system to provision and manage access to resources.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that access control systems protect information resources; rules for access have been established by	No Relevant Exceptions Noted

		the information or application owner or manager Interviewed the VP of IT and determined that Sayers relies on Active Directory and Entra ID for authentication and authorization Observed the results of a scan from the domain controller in the organization's environment and verified that the organization completes the following: • Uses groupings including security groups for validity of access for users • Creates access credentials to protected assets and data and manages the access granted to those credentials • Establishes group policies to enforce access control settings on all domain joined endpoints • Identifies and manages the inventory of users and endpoints through the use of this primary domain	
CC6.1.3	The organization maintains and enforces account credential policies, including policies for password complexity.	Reviewed the Password Policy (dated October 15, 2024) and verified the following: • The organization establishes rules for logical access credential controls for all organization-related accounts • Password complexity is established as a requirement for password creation including the use of a unique password and the construction of a password with eight or more characters, not contain personally identifiable information (PII), not contain patterns (repetitive or sequenced), and not be easily guessable using frequently used words of phrases • The password should never be shared or used on a personal account	No Relevant Exceptions Noted

		• A password rotation and expiration cadence are established where five passwords are remembered with a 180-day expiry • A password change is required if a password is deemed to be breached • Storage of passwords in a password management system is required for "emergency" management access accounts Interviewed the VP of IT and determined the following: • Passwords for new users are provided by the VP of IT during onboarding and expire upon first login • Passwords must consist of at least eight characters and expire every 180 days • Active Directory password complexity requirements are enabled, and the last five passwords cannot be re-used • In the event a password is forgotten or is expired employees can use the Microsoft Self Service Password Reset (SSPR) to reset their passwords • Users must have provided answers for security questions during onboarding; the answers to security questions and their MFA device are used to validate their identity Observed the domain default password policy from the audit scans and verified that the password settings are set to eight characters minimum, a password history of five remembered passwords, using non-reversible passwords, password complexity enabled, and a maximum password age of 180 days; this ensures that the organization manages the identification and authentication of all accounts	

CC6.2	Prior to issuing system credentials and granting system access, the entity registers and authorizes new internal and external users whose access is administered by the entity. For those users whose access is administered by the entity, user system credentials are removed when user access is no longer authorized.		
CC6.2.1	The organization revokes user access upon termination.	Interviewed the VP of IT and determined that user accounts are disabled via email to the Senior VP of HR; these are picked up by the VP of IT or the Senior Application Developer for implementation to disable access Observed the termination process including removal of access, disablement of account, and return of equipment to the organization for a sample of terminated employees (3 of 21) and verified that the organization reviews credential validity, removes physical devices, and prevents use of credentials that are no longer valid	No Relevant Exceptions Noted
CC6.2.2	The organization requires access approval and user authorization prior to access provisioning.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that access is granted upon request from a user's manager; initial requests for a connection or session are subject to authorization Interviewed the VP of IT and determined that user accounts are requested via email to the Senior VP of HR; these are picked up by the VP of IT or the Senior Application Developer for implementation Observed email requests for a sample of employees hired during the audit period (4 of 42) and verified that the Senior VP of HR receives requests for user accounts that identify the user's full name, start date, and role	No Relevant 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.		

CC6.3.1	The organization provisions role-based access to users according to the principle of least privilege.	Interviewed the VP of IT and determined that role-based security groups have been created to provide access to employees based on their position Observed Active Directory group membership for a sample of existing employees (17 of 179) and verified that each user account's security groups are role-based and provide access appropriate for each user's role Observed the use of Active Directory users and groups and verified that the organization identifies and authenticates users and applications, assigning roles and permissions using group and domain policies; the organization restricts access based upon role need and the principle of least privilege	No Relevant Exceptions Noted
CC6.4	The entity restricts physical access to facilities and protected information assets (for example, data center facilities, backup media storage, and other sensitive locations) to authorized personnel to meet the entity's objectives.		
CC6.4.1	The organization maintains and enforces procedures for the identification and documentation of visitors to its physical office facilities.	Reviewed the Sayers Information Security Policy and verified that the policy establishes employee requirements such as challenging unknown personnel found within the organization offices (including visitor procedures) Interviewed the VP of IT and determined that the Willis Tower office relies upon the building management's visitor management system; the Vernon Hills, Walpole, Clearwater, and Rosemont offices allow visitors to knock on the office suite doors for access, and paper visitor logs capture each visitor's name, company, person visiting, and date/time in and out Observed visitor procedures during physical walkthrough of Rosemont, IL, office and verified that visitors must knock at the suite door to summon an employee to open the front door and visitors are directed	No Relevant Exceptions Noted

		to a visitor log to sign in/out Observed visitor procedures during a virtual walkthroughs of the Vernon Hills, IL, Chicago, IL, (Willis Tower), and Boston, MA, (Walpole) locations and verified that visitors must sign in on a paper or electronic visitor log and are escorted by an employee for the duration of their visit Observed visitor logs at each Sayers office and verified that visitor logs are retained for at least one year and capture the visitor's name, company, phone number, and in/out date and time	
CC6.4.2	The organization maintains an alarm system within its office facilities to monitor for and alert on unauthorized access.	Interviewed the VP of IT and determined that all intrusion alarm monitoring services will alert the Sayers team members via phone call in the event an alarm is triggered Observed the burglar alarms in place at the Vernon Hills, IL, Boston, MA, (Walpole), and Tampa, FL, (Clearwater) locations and verified that they include intrusion alarms with glass break, motion, and door sensors Observed the Securitas Installation and Service Agreement, dated February 3, 2023, and a Securitas recurring invoice, dated September 2, 2024, and verified that the alarm system is active and monored in at the Vernon Hills location	No Relevant Exceptions Noted
CC6.4.3	Key logs are maintained to document and track hard keys used to access physical office locations.	Interviewed the VP of IT and determined that the Walpole and Clearwater offices use hard keys, and the Walpole suite door is unlocked during normal business hours and the Clearwater suite door is locked at all times Observed the physical key log and verified that manual hard key inventories are maintained by the office manager for the sites	No Relevant Exceptions Noted

		without centralized access control for sites, which includes the following: • Boston, MA (Walpole) • Tampa, FL (Clearwater) • Vernon Hills, IL Observed the key log and verified that it identifies the office primary contact, office location, physical keyholder name, active employee, and date provided	
CC6.4.4	The organization maintains a physical access control system to restrict access to its physical office facilities.	Interviewed the VP of IT and determined the following: • The Rosemont and Vernon Hills suite doors are locked and are managed by ACS Trilogy access control, hosted on an Azure server virtual machine • The Willis Tower suite door is locked at all times and is managed by a S2 Netbox access control system • Access control badges are provided to new hires who will be working from or visiting offices; access is requested from the Sr. Vice President of Human Resources and is configured in the appropriate access control system by the Sr. Application Developer or VP of IT • Access is based on the doors and hours employees require access to and access is revoked upon a request Observed the use of the ACS access control system, hosted on an internal server virtual machine, and verified that the system provides access control for the Vernon Hills, IL, and Rosemont, IL, sites and cardholders are named for the employee or the after-hours cleaning crew Observed the use of the S2 Netbox access control system for the Willis Tower site and verified that access control badges provided by	No Relevant Exceptions Noted

		building management are provisioned within S2 to provide access to the office suite, and cardholders are named for the employee and include the employee's picture	
CC6.4.5	The organization appropriately secures sensitive networking closets within its physical office locations.	Observed the following access controls employed for the network closets at each Sayers office and verified that appropriate security controls are in place: • Vernon Hills, IL: Network closet secured with lock and PIN • Chicago, IL (Willis Tower): Network closet secured with lock and hard key • Boston, MA (Walpole): Network closet secured with lock and PIN • Tampa, FL (Clearwater): Network closet secured with lock and hard key • Rosemont, IL: Network closet secured with lock and hard key	No Relevant Exceptions Noted
CC6.4.6	The organization maintains video surveillance systems to monitor its physical office locations and retains footage for review.	Observed the surveillance systems at the Vernon Hills, IL, and Boston, MA, (Walpole) locations and verified that cameras are in place to provide coverage of entrances and exits and recording is based on motion; video is stored locally on camera SD cards and is uploaded to cloud-based storage for 30 days and full access to live/recorded video is limited to the VP of IT Observed the surveillance systems at the Chicago, IL, (Willis Tower), Tampa, FL, (Clearwater), and Rosemont, IL, locations and verified that the systems are provided by the building and provide coverage of entrances and exits; footage is available upon request	No Relevant 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.		

CC6.5.1	Physical media is secured and destroyed when no longer needed using shredders and certified destruction agencies.	Interviewed the VP of IT and determined that each office is equipped with at least one small office cross-cut shredder that is emptied as needed; the Clearwater office annually contracts with a shredding vendor to shred old files on site Observed the following office spaces and verified shredders and shred bins were in place at each: • Vernon Hills, IL • Chicago, IL (Willis Tower) • Boston, MA (Walpole) • Tampa, FL (Clearwater) • Rosemont, IL Reviewed the Sayers Information Security Policy and verified the following: • Paper media containing operational or confidential information no longer needed must be shredded before disposal • All remote employees or representatives of the organization must have direct access to a shredder • All external media must be sanitized or destroyed and any media containing operational or confidential information must not be disposed of in a waste container • External media must be returned to a supervisor and wiped clean of data • The Vice President of Information Technology oversees this wipe procedure and once wiped, a certified destruction agency must handle the media destruction and disposal	No Relevant Exceptions Noted
CC6.5.2	The organization retains data appropriately according to its sensitivity and destroys data upon expiration of its retention period.	Reviewed the Sayers Data Retention Policy and verified that data is destroyed upon expiration of its retention period unless a legitimate business reason exists for maintaining it; exceptions to the policy must be approved by	No Relevant Exceptions Noted

		Sayers Data Protection Officer with consultation of legal counsel Observed the ShareFile client folder deletion reports for folder purges occurring between February 10, 2025, through March 28, 2025, and April 3, 2025, through May 28, 2025 and verified that the reports track the files and folders deleted, the user initiating the purge, user's public IP address, and event ID	
CC6.6	The entity implements logical access security measures to protect against threats from sources outside its system boundaries.		
CC6.6.1	Firewalls are maintained to restrict traffic across networks.	Interviewed the VP of IT and Sr. Application Developer and determined the following: • The VP of IT reviews the firmware versions on Palo Alto firewalls and Aruba network switches monthly and compares them to the most recent releases; the firewalls and switches are updated to the most recent stable version, normally when a new major version is released • Rules are reviewed and validated annually • The Azure virtual Palo Alto firewall is configured to permit traffic based on port and protocol to the appropriate server Observed the use of the Imperva web application firewall (WAF) and verified that protected public hosts include www., info., mail., portal., events., and portalapi.sayers.com; reported statistics include bandwidth over 30 days, number of human visits, number of bot visits, number of WAF sessions, and status	No Relevant Exceptions Noted
CC6.6.2	The organization encrypts data at rest using drive, device, and server-side encryption.	Interviewed the VP of IT and determined the following about encryption of data at rest: • Workstation drives are encrypted using BitLocker for	No Relevant Exceptions Noted

		Windows and File Vault for Macs • Full device encryption is required for Bring Your Own Device (BYOD) devices • Encryption is enforced using Intune policy settings • All servers are hosted in Azure as VMs and use default server-side encryption with Azure managed keys Observed encryption on a sample of MacOS workstations (3 of 17), Windows workstations (9 of 101), and Azure VMs (5 of 67) and verified that encryption is appropriately enabled	
CC6.6.3	The use of MFA is enforced for all normal users, privileged users, and for VPN connections.	Reviewed the Password Policy (dated October 15, 2024) and verified that MFA is highly encouraged and required for applications potentially containing confidential information Interviewed the VP of IT and determined that Entra ID Conditional Access rules enforce MFA for all normal users, privileged users and for Absolute VPN connections Observed examples of remote logins via Microsoft 365 web-based access to Sayers resources and via Absolute VPN and verified that both require Entra ID SSO with MFA Observed Entra ID Conditional Access Policies and verified that Sayers uses a conditional access rule to force MFA for all resources and for all users; policies are in place that require MFA for: • Azure VPN • Risky sign-ins • Admin Portal • Admin accounts • User accounts	No Relevant 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.		

CC6.7.1	The organization maintains and enforces mobile device management procedures for employee devices.	Interviewed the VP of IT and Sr. Application Developer and determined that Sayers allows users to use their personal mobile device to access Microsoft 365 sources and Intune policies are applied to these devices; mobile devices must not be jailbroken or rooted, must have full device encryption, and must have a screen timeout enabled Reviewed the Sayers Information Security Policy and verified that the policy establishes employee requirements such as locking of unattended computers and work from home equipment use	No Relevant Exceptions Noted
CC6.7.2	The organization requires the encryption of data in transit according to industry-accepted cryptographic algorithms.	Interviewed the VP of IT and determined the following about encryption of data in transit: • Site to site virtual private networks (VPNs) are established through the Palo Alto firewalls at each site • Sayers uses a hub-and-spoke model where every office is a spoke that connects to the Azure hub • Sayers offices can only communicate with Azure; they are not configured to pass traffic directly to another site or via Azure • Laptops use the Absolute VPN client that encrypts traffic via a symmetric AES-256-bit key • Login sessions to Entra ID, Palo Alto firewall consoles, network switch consoles, and tools such as Sentinel One are secured with HTTPS or Transport Layer Security (TLS) 1.2 Observed the Absolute VPN client encryption settings and verified that AES-256 is enabled for secure access to Sayers networks	No Relevant 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.		

CC6.8.1	The organization requires the installation of up-to-date antivirus and anti-malware software on all endpoints.	Interviewed the VP of IT and the Senior Application Developer and determined the following: • Sayers primarily uses SentinelOne as an antivirus platform, with some systems remaining on the legacy Cylance Aurora platform • Endpoint agents are installed on all servers and workstations and are configured for automatic updating and tamper protection • Settings deployed to systems allow the agents to detect and protect systems with centralized alerting and logging • Agents are installed upon enrollment in Intune Observed Cylance Aurora and verified that it is used for malware protection with auto-quarantine, process termination, and script protection; memory protection includes RAM scraping, malicious payload, and stack project, and agents update automatically Observed SentinelOne settings and policies for Windows, MacOS, and Linux endpoints and verified the following: • Endpoints update automatically • Removable storage is blocked • Protection from malicious threats and detection for suspicious threats is enabled • Enabled detections include static and behavioral threats, documents, scripts, lateral movement, fileless, PUA, and interactive threats Observed a sample of Windows workstations (10 of 101) and verified that each is protected with Cylance or SentinelOne Observed a sample of MacOS workstations (3 of 17) and a	No Relevant Exceptions Noted

		sample of Azure Windows VMs (5 of 67) and verified that each is protected with SentinelOne Observed antivirus update settings and verified that Cylance Aurora agents update automatically, and SentinelOne updates occur automatically Observed threat reports from the Cylance and SentinelOne endpoint detection and response solutions and verified that the organization has implemented antivirus and anti-malware software in its environment, which scans on demand; the results of scans performed are saved in an exportable report Observed threat reports from the audit period from Cylance and SentinelOne and verified that the organization has implemented antivirus and anti-malware software in its environment	

System Operations

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC7.1	To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.		
CC7.1.1	The organization undergoes internal and external vulnerability scanning to identify vulnerabilities and threats to be remediated.	Reviewed the Vulnerability Management Policy (dated January 29, 2025) and verified that the VP of IT and a designated team is authorized to conduct vulnerability scans on systems, devices, and applications connected to organizational networks Interviewed the VP of IT and the Senior Application Developer and determined the following: • Internal vulnerability scans are conducted weekly by Rapid7 using a combination of Rapid7 endpoint agents • Findings are reviewed by the IT Subcommittee, which prioritizes them for remediation and creates change requests for implementation • External vulnerabilities are identified through the use of BitSight and Security Scorecard • These reports are also reviewed by the IT Subcommittee • Rapid7 agents are installed via Group Policy on servers and Intune for workstations Observed monthly Rapid7 scans for a sample of months during the audit period (3 of 12) and verified that high risk reports include vulnerability information from Rapid7 internal scans and agent reporting; vulnerability reports include vulnerabilities by severity, severity trends, and risk score Observed Rapid7 monthly executive summary reports from during the audit period and	No Relevant Exceptions Noted

		verified that they identify the total number of assets, the total vulnerabilities and critical vulnerabilities, and vulnerability remediation over the previous 30 days Observed the Security Scorecard for Sayers and verified that ratings are given for cubit score, DNS health, endpoint security, IP reputation, and network security Observed Security Scorecard history and verified that public score has been tracked from August 2024 to July 2025	
CC7.1.2	The organization undergoes annual penetration testing of all public IP addresses used by Sayers assets.	Interviewed the VP of IT and determined that Sayers conducts penetration testing annually on the public IP addresses in use at each Sayers office and Azure; Phalanx conducts penetration testing, and reports are reviewed by the IT Committee Observed a Phalanx Security external network penetration test report from during the audit period and verified that scope includes all public IP addresses used by Sayers assets, and methodology involves adversarial mindset using tactics, techniques, and procedures used by real attackers; two minor findings were identified	No Relevant Exceptions Noted
CC7.2	The entity monitors system components and the operation of those components for anomalies that are indicative of malicious acts, natural disasters, and errors affecting the entity's ability to meet its objectives; anomalies are analyzed to determine whether they represent security events.		
CC7.2.1	The organization has implemented monitoring tools to monitor and alert on the security of its networks and systems, and logs are reviewed periodically.	Reviewed the Log Review Policy (dated May 1, 2025) and verified that the organization identifies logs to review from network peripherals and equipment where, by policy, logs are reviewed once a quarter at a minimum or once per month based on categorization Interviewed the VP of IT and the Senior Application Developer and determined that each Palo Alto	No Relevant Exceptions Noted

		firewall is licensed with security services that block malicious files and intrusion attempts; Palo Alto logs are ingested by Rapid7 for additional analysis and alerting Observed the following examples of monitoring alerts to verify that Sayers has appropriate network monitoring tools in use throughout the environment and regularly receives alerts: • InsightIDR investigation for password resets, dated June 4, 2025 • InsightIDR investigation for suspicious authentication, dated June 1, 2025 • Office365 DLP alert, dated February 25, 2025 • Cylance Aurora Endpoint Defense alert, dated April 15, 2025 • SentinelOne incident status and analysis verdict updates, dated April 21, 2025 Observed the Citrix ShareFile access log for the time period of March 8, 2025, through June 6, 2025, and verified that the logs capture the timestamp, action, folder name and path, user and email address, source IP address, and activity type for each event	
CC7.3	The entity evaluates security events to determine whether they could or have resulted in a failure of the entity to meet its objectives (security incidents) and, if so, takes actions to prevent or address such failures.		
CC7.3.1	The organization investigates alerts of potential security incidents and takes appropriate action.	Reviewed the Sayers Information Security Policy and verified the following: • Reporting security incidents is the responsibility of each employee/contractor and all incidents are escalated to IT • Incidents are logged, investigated, and remediated and suspected criminal action is reported to law enforcement by the VP of IT • Security breaches of secure information, networks, or systems are reported through	No Relevant Exceptions Noted

		an internal IT email address or by calling/contacting a member of IT Reviewed the Sayers Incident Response Policy and verified it identifies the following: • The five phases of incident response, including prepare, detect, respond, recover, post-incident review • Contact table identifying the IT Committee as the IR Team with support from Operations & Communications and Information Technology team leads • The requirement for the incident response plan to be subject to an annual review and update as needed or upon significant infrastructure changes Interviewed the VP of IT and the VP of Project Management and determined the following: • Sayers prepares for incidents by ensuring employees complete Security Awareness Training that includes guidance on reporting potential incidents to IT • Reported or detected events are investigated to determine if they are false positives or if they rise to the level of an incident that requires activation of the Incident Response Plan • In the event of an actual incident, the plan is activated Observed the following examples of monitoring alerts to verify that Sayers has appropriate network monitoring tools in use throughout the environment and regularly receives alerts: • InsightIDR investigation for password resets, dated June 4, 2025	

		• InsightIDR investigation for suspicious authentication, dated June 1, 2025 • Office365 DLP alert, dated February 25, 2025 • Cylance Aurora Endpoint Defense alert, dated April 15, 2025 • SentinelOne incident status and analysis verdict updates, dated April 21, 2025	
CC7.4	The entity responds to identified security incidents by executing a defined incident response program to understand, contain, remediate, and communicate security incidents, as appropriate.		
CC7.4.1	The organization responds to identified security incidents following a formally defined incident response plan.	Reviewed the Sayers Information Security Policy and verified the following: • Reporting security incidents is the responsibility of each employee/contractor and all incidents are escalated to IT • Incidents are logged, investigated, and remediated and suspected criminal action is reported to law enforcement by the VP of IT • Security breaches of secure information, networks, or systems are reported through an internal IT email address or by calling/contacting a member of IT • Sayers notifies the affected parties via email to communicate the method, date/time of breach, the impact, how it affects the client, measures taken to remediate effects, and measures taken to prevent future breaches • The VP of IT or appropriate personnel distribute security reminders addressing topics, including incident identification and response Reviewed the Sayers Incident Response Policy and verified it identifies the following: • The five phases of incident response, including prepare,	No Relevant Exceptions Noted

		detect, respond, recover, post-incident review • Contact table identifying the IT Committee as the IR Team with support from Operations & Communications and Information Technology team leads • The requirement for the incident response plan to be subject to an annual review and update as needed or upon significant infrastructure changes Interviewed the VP of IT and the VP of Project Management and determined the following: • In the event of an actual incident, the IT Committee serves as the Incident Response team • Incidents are entered into the IT incident response tracker spreadsheet • All activity pertaining to the incident, including responses and timelines, is recorded • The Incident Response team reviews the ongoing incident and determines the best course to contain or eliminate the impact of the incident on operations • Opportunities for improvement are identified following incidents Observed the Incident Response team listed in the Incident Response Policy and verified that the IT Committee is identified as the Incident Response team with support from Operations and Communications and IT Team Leads as needed	
CC7.5	The entity identifies, develops, and implements activities to recover from identified security incidents.		
CC7.5.1	The organization patches all systems on a routine basis.	Reviewed the Vulnerability Management Policy (dated January 29, 2025) and verified that the policy identifies procedures for	No Relevant Exceptions Noted

		patching and remediation of vulnerabilities Observed a sample of Azure workstation VMs (5 of 67), a sample of Windows workstations (9 of 101), and a sample of MacOS workstations (3 of 17) in use during the audit period and verified that patching was performed monthly on all sampled systems	

Change Management

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC8.1	The entity authorizes, designs, develops or acquires, configures, documents, tests, approves, and implements changes to infrastructure, data, software, and procedures to meet its objectives.		
CC8.1.1	All changes within the environment require a request, assignment, and approval.	Interviewed the VP of IT and Sr. Application Developer and determined that change requests are reviewed by the IT Subcommittee to determine if the change has a significant impact; change requests are tracked in a spreadsheet Reviewed the Sayers Change Management Policy and verified the following: • Change requests must document importance, urgency, and impact; date of submission and of change implementation; change owner; nature of the change; roll-back plan; approver; implementor; and final result (success or failure) • Changes with significant impact must be scheduled • Resource owners must be notified of changes • Complex changes are tested for impact on usability and security • Changes must be approved by the VP of IT, IT Subcommittee, or IT Committee Observed a spreadsheet that is used to track changes completed within the organization's environment and verified that all changes require a request, assignment, and approval; changes also require post-implementation testing and a regression plan as a contingency for failure	No Relevant Exceptions Noted
CC8.1.2	Changes driven by identified vulnerabilities are tracked using the change management process.	Interviewed the VP of IT and Sr. Application Developer and determined that changes driven by identified vulnerabilities are	No Relevant Exceptions Noted

		tracked using the change management process Observed the Sayers IT change control tracker spreadsheet and verified security changes, including vulnerability mitigation and upgrades, are tracked through the change management process	
CC8.1.3	Defined hardening and configuration standards are implemented on the organization's end user workstations and devices.	Reviewed the Sayers Server Hardening Policy and verified the following: • Hardening steps include installing OS from a trusted source; installing patches and updates; removing vulnerable software, services, and functionality; and installing local firewalls, antivirus, file permissions, logging, Active Directory group policy settings, and Rapid7 and SentinelOne agents • Servers adhere to NIST 800-53 Section 5.3 configuration requirements • Configuration changes are formally reviewed, approved, and documented Interviewed the VP of IT and Sr. Application Developer and determined the following: • Sayers uses Windows and Macs for end user workstations and devices are enrolled in Intune where device policies install SentinelOne and Rapid7 agents and apply screen timeout and lock settings • BitLocker is enforced on Windows workstations and File Vault enabled on Macs • Windows systems are joined to Active Directory, where Group Policy templates that align with NIST 800-53 are selectively applied; settings that impede functionality are not implemented	No Relevant Exceptions Noted

Risk Mitigation

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
CC9.1	The entity identifies, selects, and develops risk mitigation activities for risks arising from potential business disruptions.		
CC9.1.1	The organization develops risk treatment strategies for risks resulting from business disruptions, including risk transference and risk mitigation controls.	Reviewed the Sayers Information Security Policy (dated October 24, 2024) and verified that security measures to address risks are identified with timeline, costs, and ownership Interviewed the VP of IT, the Senior VP of Solutions, and the VP of Project Management and determined that existing controls to reduce risk are discussed, and additional controls are planned Observed the risk register and treatment plan and verified that the register tracks percent of mitigation for risk, as well as risk treatment details Observed the Certificate of Liability Insurance for Sayers Technology Holdings, Inc., Sayers Technology Services, LLC, and Sayers Technology, LLC and verified that coverage provided includes: • Commercial general liability • Automobile liability • Umbrella liability • Workers' compensation	No Relevant Exceptions Noted
CC9.2	The entity assesses and manages risks associated with vendors and business partners.		
CC9.2.1	New vendors are vetted prior to engagement and IT personnel maintain a list of IT vendors impacting financial and/or confidential data.	Interviewed the VP of IT and VP of Project Management and determined the following related to vendor management: • Sayers tracks vendors using a Smartsheet spreadsheet • New vendors are requested by business units or departments and are vetted in conjunction with IT • Requests for new vendors are discussed during IT Subcommittee meetings,	No Relevant Exceptions Noted

		where the vendor, services provided, and the criticality of the vendor are reviewed; audit reports are reviewed, if provided • Vendor access limitations are discussed for vendors with potential access to sensitive information Reviewed the Sayers Vendor Management Policy and verified that IT personnel maintain a list of IT vendors impacting financial and/or confidential data Observed the Sayers Vendor Tracking - Responsibilities & Compliance spreadsheet and verified that the following metrics are tracked by vendor: • Vendor name • Service provided • Access to financial/confidential information • NDA in place • Contract in place • Service provider's and Sayers' responsibilities • Completion of onboarding risk assessment • URL to compliance trust center • Target review date • Date of last review • Notes	
CC9.2.2	Third parties and vendors are reviewed annually to ensure their continued compliance with the organization's requirements.	Interviewed the VP of IT and VP of Project Management and determined that vendors on the vendor tracking sheet are reviewed annually by the Sr. Vice President-Solutions, who is the owner of the document and is responsible for maintenance; due dates for annual vendor reviews are tracked, along with the type of audit report provided and/or a link to the vendor's online trust center where reports can be securely downloaded	No Relevant Exceptions Noted

		Reviewed the Sayers Vendor Management Policy and verified that third-party service providers compliance is to be monitored via third-party SOC reports or equivalent, and management must regularly review vendors Observed evidence of compliance reviews for a sample of 3 of 4 critical service providers and verified that all vendor reviews are tracked and annual reviews were conducted within the audit period Observed the Sayers Vendor Tracking - Responsibilities & Compliance spreadsheet and verified that the following metrics are tracked by vendor: • Vendor name • Service provided • Access to financial/confidential information • NDA in place • Contract in place • Service provider's and Sayers' responsibilities • Completion of onboarding risk assessment • URL to compliance trust center • Target review date • Date of last review • Notes	
CC9.2.3	Appropriate documentation is maintained with the organization's vendors and service providers to address compliance with legal and regulatory requirements, confidentiality, and non-disclosure requirements.	Reviewed the Sayers Vendor Management Policy and verified that SLAs are considered when negotiating agreements with vendors, and contracts and service agreements must be in place to address vendor compliance with legal and regulatory requirements Observed service provider agreements for a sample of 3 of 4 critical service providers and verified that they include end user agreements and master services agreements, include confidentiality and non-disclosure language, and	No Relevant Exceptions Noted

		identify protections for customer data	

Additional Criteria for Availability

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
A1.1	The entity maintains, monitors, and evaluates current processing capacity and use of system components (infrastructure, data, and software) to manage capacity demand and to enable the implementation of additional capacity to help meet its objectives.		
A1.1.1	The organization routinely reviews aggregated logs to identify issues related to system use.	Reviewed the Sayers Log Review Policy (dated May 1, 2025) and verified that the organization identifies logs to review from network peripherals and equipment where, by policy, logs are reviewed once a quarter at a minimum or once per month based on categorization Interviewed the VP of IT and determined that logs are ingested from multiple sources, and logs are sent to the VP of IT and the Senior Application Developer for investigation Observed Citrix ShareFile access logs and verified that the following is captured for each event: time stamp, action, folder name and path, user and email address, source IP address, and activity type	No Relevant Exceptions Noted
A1.2	The entity authorizes, designs, develops or acquires, implements, operates, approves, maintains, and monitors environmental protections, software, data backup processes, and recovery infrastructure to meet its objectives.		
A1.2.1	The organization maintains offices equipped with building-supplied fire detection and suppression systems and alternative power supplies.	Interviewed the VP of IT and determined that each Sayers office is a leased space within an office building with life safety systems provided by the property manager: fire detection and alarms, fire suppression systems, emergency lighting, and testing of these systems; offices have uninterruptible power supplies (UPS) in the network closet for firewalls and network switches Observed life safety systems at Sayers offices and verified that fire detection and alarm systems with smoke detectors, strobes,	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		and sirens, as well as annually inspected fire extinguishers, are provided by building management and present within the following Sayers offices: • Vernon Hills, IL • Chicago, IL • Boston, MA • Tampa, FL • Rosemont, IL	
A1.2.2	The organization maintains defined procedures to ensure the continuation of business processes and recovery of critical systems in the event of a disaster or loss.	Reviewed the Business Continuity Plan (dated April 29, 2025) and verified that the organization has established policies and procedures to support contingency planning controls; the plan outlines the following: • In-scope locations, as well as responsibilities and priorities • Instances in which the plan would be triggered and procedures for continuity and recovery efforts • Business recovery processes and responsible parties • Processes and procedures for both administrative and technical incidents • Procedures for testing the plan Interviewed the VP of IT and the COO and determined that a business continuity plan is maintained that identifies teams responsible for execution of the plan, teams who provide support for the plan, an identifies priorities to observe in during a disruptive incident; step-by-step guidance is provided to the Business Continuity team that identifies the person responsible, when the action should be carried out, and details on what to do, and similar guidance is provided for the Business Recovery Process to establish an alternate location and resources to restore normal functionality	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
A1.2.3	The organization creates backups of data based on defined schedules and retains backups according to backup frequency.	Reviewed the Sayers Data Backup Policy (dated October 16, 2024) and verified that backup and backup retention schedules are defined Interviewed the VP of IT and determined the following: • Sayers servers are hosted on Azure virtual machines (VMs), which are backed up and stored by Azure Backup, with backup sets stored in a recovery vault • Backup retention is determined by frequency of backup • Individual backup jobs are created for each backed up server • Recovery vaults use Azure-managed encryption • Emailed backup alerts are monitored by the VP of IT and the Senior Application Developer for failures Observed backup settings and verified that the organization creates data backups based on data priorities and classifications; the backup settings are set to perform recurring backups with retention periods that conform with data retention requirements, and backups are performed using the Azure backup utility	No Relevant Exceptions Noted
A1.3	The entity tests recovery plan procedures supporting system recovery to meet its objectives.		
A1.3.1	The organization completes routine testing of its business continuity and disaster recovery procedures using tabletop exercises.	Reviewed the Business Continuity Plan (dated April 29, 2025) and verified that the organization maintains business continuity and disaster recovery procedures and requirements for testing these procedures Interviewed the VP of IT and the COO and determined that tabletop exercises are conducted to present Business Continuity and	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		Disaster Recovery teams with a disruptive event and the resulting impact on Sayers operations, with a focus on five specific potential scenarios; the ability to recover from an Azure-related incident is validated through testing backup restoration Observed backup and restoration testing from during the audit period and verified that the organization tests the integrity and completeness of backups performed on its environments in support of its disaster recovery efforts; backups were performed and recovered without incident for both tests conducted during the audit period Observed notes and the calendar invite for business continuity testing conducted during the audit period and verified that the organization implements and practices business continuity procedures through testing	
A1.3.2	The organization performs backup restoration testing at least annually.	Reviewed the Sayers Data Backup Policy (dated October 16, 2024) and verified that backup restoration testing is performed at least annually; actual restores conducted during maintenance of systems are considered tests, and test restores are tracked via the change management process Interviewed the VP of IT and determined that test restores are conducted annually to validate backups; during the audit period, two successful backup restoration tests were performed: one VM was restored and powered on, and a second test was of a file-level restore Observed data backup test restore reports dated August 14, 2024, and May 12, 2025, for tests of file-level backups and VM backups and	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
		verified that reports track the date, objective, and results of the test; both tests were successful	

Additional Criteria for Confidentiality

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
C1.1	The entity identifies and maintains confidential information to meet the entity's objectives related to confidentiality.		
C1.1.1	Sayers retains data as needed to conduct business activities and comply with applicable laws and regulations.	Reviewed the Sayers Data Retention Policy and verified that data is only retained when it is necessary to effectively conduct business activities, fulfill the mission, and comply with applicable laws and regulations Reviewed the Sayers Information Security Policy and verified that the policy establishes retention of ownership of assets and software developed/generated while employed	No Relevant Exceptions Noted
C1.1.2	Data classifications are used to drive guidelines for the storage, transmission, consumption, and destruction of company data.	Reviewed the Sayers Data Classification & Confidential Data Policy and verified that data classifications include public, operational, and confidential and guidance for the storage, transmission, consumption, and destruction of each category is provided	No Relevant Exceptions Noted
C1.2	The entity disposes of confidential information to meet the entity's objectives related to confidentiality.		
C1.2.1	Sayers data is destroyed upon expiration of its retention period.	Reviewed the Sayers Data Retention Policy and verified that data is destroyed upon expiration of its retention period unless a legitimate business reason exists for maintaining it; exceptions to the policy must be approved by Sayers Data Protection Officer with consultation of legal counsel Observed the ShareFile client folder deletion reports for folder purges occurring between February 10, 2025, through March 28, 2025, and April 3, 2025, through May 28, 2025 and verified that the reports track the files and folders deleted, the user initiating the purge, user's public IP address, and event ID	No Relevant Exceptions Noted

Ctrl #	Description of Controls	Service Auditor's Tests of Controls	Test Results
C1.2.2	Policies and procedures are in place to destroy confidential information that has been identified for destruction.	Observed the following office spaces and verified shredders and shred bins were in place at each: • Vernon Hills, IL • Chicago, IL (Willis Tower) • Boston, MA (Walpole) • Tampa, FL (Clearwater) • Rosemont, IL Reviewed the Sayers Information Security Policy and verified the following: • Paper media containing operational or confidential information no longer needed must be shredded before disposal • All remote employees or representatives of the organization must have direct access to a shredder • All external media must be sanitized or destroyed and any media containing operational or confidential information must not be disposed of in a waste container • External media must be returned to a supervisor and wiped clean of data • The Vice President of Information Technology oversees this wipe procedure and once wiped, a certified destruction agency must handle the media destruction and disposal	No Relevant Exceptions Noted