360 ADVANCED

SOC 3® REPORT ON CONTROLS RELEVANT TO SECURITY, AVAILABILITY, AND CONFIDENTIALITY FOR SENSITIVE DATA PLATFORM™ SERVICES

SPIRION, LLC

MARCH 1, 2021 TO FEBRUARY 28, 2022

SPIRION™

AICPA SOC
aicpa.org/soc4so
SOC for Service Organizations | Service Organizations
™

SPIRION, LLC

Table of Contents

SECTION 1:

INDEPENDENT SERVICE AUDITOR'S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To Spirion, LLC:

Scope

We have examined Spirion, LLC's ("Spirion") assertion included in Section 2 of this report that the controls within Spirion's Sensitive Data Platform™ system were effective throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance that Spirion'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*).

Spirion uses sub-service organizations for cloud hosting and security monitoring services. Spirion's assertion and description of the boundaries of the Sensitive Data Platform™, included in Section 2 and Section 3 of this report, respectively, indicate that certain applicable trust services criteria can only be met if certain types of controls at the aforementioned sub-service organizations are suitably designed and operating effectively. The description does not include any of the controls expected to be implemented at the sub-service organizations. Our examination did not extend to the services provided by the sub-service organizations, and we have not evaluated whether the controls management expects to be implemented at the sub-service organizations have been implemented or whether such controls were suitability designed and operating effectively throughout the period March 1, 2021 to February 28, 2022.

Service Organization's Responsibilities

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

Service Auditor's Responsibilities

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

Our examination included:

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

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

Inherent Limitations

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

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

Opinion

In our opinion, management's assertion that the controls within Spirion's Sensitive Data Platform™ system were effective throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance that Spirion's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects.

April 11, 2022
St. Petersburg, Florida

SECTION 2:

MANAGEMENT'S ASSERTION

MANAGEMENT'S ASSERTION

April 11, 2022

We are responsible for designing, implementing, operating, and maintaining effective controls with Spirion, LLC's ("Spirion") Sensitive Data Platform™ system throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance that Spirion's service commitments and system requirements relevant to Security, Availability, and Confidentiality were achieved. Our description of the boundaries of the system is presented in Section 3 of this report and identifies the aspects of the system covered by our assertion. Spirion uses sub-service organizations for cloud hosting and security monitoring services. The description included in Section 3 excludes the applicable trust services criteria and related controls of the sub-service organizations.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance the Spirion's service commitments and system requirements were achieved based on the trust services criteria relevant to Security, Availability, and Confidentiality set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy* (AICPA, *Trust Services Criteria*). Spirion's objectives for the system in applying the applicable trust services criteria are embodied in its service commitments and system requirements relevant to the applicable trust services criteria. The principal service commitments and system requirements related to the applicable trust services criteria are presented in Section 4 of this report.

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

We assert that the controls within the system were effective throughout the period March 1, 2021 to February 28, 2022, to provide reasonable assurance that Spirion's service commitments and system requirements were achieved based on the applicable trust services criteria.

/s/ Spirion, LLC

Chris Thomley – Chief Financial Officer

Scott Giordano – VP Corporate Privacy and General Counsel

SECTION 3:

DESCRIPTION OF THE BOUNDARIES OF THE SYSTEM

OVERVIEW OF OPERATIONS AND THE SYSTEM

Company Overview and Background

Spirion, headquartered in St. Petersburg, Florida, is a provider of enterprise data management software designed to proactively identify and minimize the risks, costs, and reputational damage of successful cyberattacks and the unauthorized access and use of confidential data. Spirion specializes in the high-precision search and automated classification of both structured and unstructured data using its AnyFind™ engine to analyze text and images. Spirion customers are generally high-growth firms across the healthcare, public sector, retail, education, financial services, energy, industrial, and entertainment markets.

Overview of Sensitive Data Platform™ Services System

The Sensitive Data Platform™ system provides organizations with a solution to analyze, respond to, and detect sensitive information in organizational environments. Hosted in Azure, the Sensitive Data Platform™ system allows users to identify locations of sensitive data in their cloud and on-premise environments using agents with automated rules to manage data and reduce the attack surface.

Sensitive Data Platform™ agents are self-contained in the platform itself, or deployed to Windows, RedHat Linux, and macOS machines. Sensitive Data Platform™ scans systems selected by customers to locate sensitive data that may not be easy to find, including forgotten documents. The system additionally assists in securing or disposing of data, thereby, protecting sensitive information from theft and / or inappropriate use.

The Sensitive Data Platform™ system provides insight into the location, risks, and vulnerabilities for an entity's data to provide a better understanding of the entity's stance on data that is protected or unprotected. Sensitive data is automatically discovered via AnyFind™ discovery algorithms. The data is then optionally classified and / or remediated, providing visibility and monitoring, thus enabling data stakeholders to easily control and consolidate sensitive data on systems, reducing an organizations sensitive data footprint and risk. There are options for customized reports and policy enforcement.

The web-based user interface allows for drill-down capabilities to understand sensitive data assets and manage risks effectively. Users can visualize how data is protected to improve the security posture, and key performance indicator (KPI) reports can be run to track ongoing management of risks.

Sub-Service Organizations and Complementary Controls

Spirion uses sub-service organizations for cloud hosting and security monitoring services. To monitor and evaluate the adequacy and effectiveness of controls in place at the sub-service organization, Spirion's management obtains and reviews the applicable Service Auditor's reports and / or compliance certifications for the sub-service organization.

Infrastructure

Sensitive Data Platform™ is hosted and managed by Spirion in its Azure cloud environment. Agents are deployed to Windows, RedHat Linux, and OSX machines, or within the Sensitive Data Platform™ cloud environment container. Spirion uses Azure data centers to host the enterprise software solution's production and non-production environments. Sensitive Data Platform™ runs on Azure clusters across multiple regions for high availability. Spirion's local user networks are distinct and isolated from the production network (Azure) in which Spirion applications and customer data are maintained. This segregation of systems access is facilitated through distinct Active Directory domains and firewall rulesets. Production systems run on high availability clusters with self-healing features.

The following describes the in-scope components supporting the Sensitive Data Platform™ system:

System / Application	Description	Infrastructure
Sensitive Data Platform™ Services	Sensitive data platform service	Microsoft Windows on Azure, Linux on Azure, SQL Server, Postgres and deployed agents

Software

Spirion's AnyFind™ engine is internally developed in a Microsoft environment. Individual customer environments are created as part of the onboarding process of new customers. Spirion personnel do not have application-level access to production data. Production troubleshooting may occur in the pre-production environment, where data is also de-identified. System operations are managed through the browser-based front-end.

People

Spirion personnel are organized into separate functional groups to provide adequate separation of duties within the information systems group and between users. The job descriptions of each functional group are reviewed on an as-needed basis dependent on changes in the strategic initiatives and skillset needs identified and communicated by management to the Human Resources Team. Functional groups include:

Innovation

The Innovation Team assesses the needs of the marketplace, including prospects and existing customers, to coordinate the process of determining the Sensitive Data Manger's product roadmap. Innovation is responsible for the Discovery phase of the software development life cycle (SDLC) and develops the product strategy and setting the product vision and specifications for the solution. The Innovation Team manages the Business Analysts and oversees the release progression as a key member of the Release Steering Committee. The Release Steering Committee monitors the delivery and quality of each iterative release.

Development

The Vice President of Engineering leads the Development Team. The Development Team consists of Cloud and Solution Architects, Developers, and Quality Assurance personnel. The Vice President of Engineering works with the Heady of Product in approving the product roadmap. Each release project is tracked in the Jira ticketing system throughout the development life cycle. Access to Jira development assigned tasks is restricted to authorized developers.

Capacity planning is integrated within the Project Management Office and Application Development processes are employed within the company to ensure necessary resources and competencies are available to achieve corporate goals. Additional systems, qualified personnel, and tools may be added as determined necessary.

Information Technology

The Information Technology Team is responsible for the maintenance, security and availability monitoring, and upkeep of the system components that reside above the virtualization layer (i.e., operating system through presentation layer). The Cloud Operations Team is also responsible for the general availability phase of the software development management and the implementation of the changes into production.

The Security Engineers report to the Vice President of IT and monitor uptime availability logs, feeds, network traffic, vulnerability status, and correlated events to identify and alert on anomalies indicative of a potential attack of the solution via both internal and external tools.

Customer Success

The Customer Support Team is responsible for troubleshooting any issues with product use or installation and providing training to new and existing customers in regard to the common rules and policy set-up actions. Customer Success is responsible for communicating existing customer feedback to the Release Steering Committee and the Product Team for future product roadmap considerations. The Vice President of IT is represented on the Release Steering Committee.

Compliance

In consultation and coordination with the V.P., Corporate Privacy, and General Counsel, the Vice President of IT is responsible for monitoring environmental, regulatory, and technological changes affecting Spirion and its systems. As needed, but at least annually, updates to controls and governance documentation are made by security personnel and approved by the Vice President of IT.

The Chief Executive Officer has assigned responsibilities for the maintenance and enforcement of security and confidentiality policies, and changes and updates to those policies, to the Vice President of IT.

The V.P., Corporate Privacy, and General Counsel, and the Vice President of IT are both members of the Product Steering Committee and provide operational compliance reporting services to all management levels of Spirion.

Procedures

Spirion's management is responsible for maintaining and implementing information technology general computer controls related to computer processing supporting the Sensitive Data Platform™ system. These controls provide the basis for reliance on information / data from the systems used by user entities.

The Corporate Information Security Policies (CISP) and the Application Security Development Program

The CISP and Application Security Development Program considers, measures, mitigates, and monitors risk to Spirion's physical and internal networks and the enterprise software solution. The CISP and Application Security Development Program are designed to achieve the following objectives:

- Ensure the security, confidentiality, integrity, and availability of information and other forms of confidential company information.
- Protect against any reasonably anticipated threats or hazards to the security or integrity of such information.
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer or individual, or to the company.
- Ensure the proper disposal of personal information, customer information, and other types of confidential information.
- Provide reasonable assurance that business objectives will be achieved, and security breaches will be prevented or detected and, when not reasonably prevented, that breaches are timely contained and corrected.
- Comply with legal, statutory, contractual, and internally developed requirements.

The CISP and Application Security Development Program institutionalize these enumerated risk control objectives through training and acknowledgement of the CISP by Spirion employees. Security Awareness Training is designed to ensure security risks are well-understood by the appropriate audiences and that

controls to prevent or limit harm to the company or its information assets are established and functioning as intended. This training is conducted for employees during onboarding and at least annually each year.

Incident Response

Annually, Spirion completes a business impact assessment (BIA) that drives the update of the Business Continuity Plan (BCP). BCP testing includes realistic scenarios and involves participation of employees from cross- functional departments to derive actual response times and actions and compare to contractual commitments and overall company objectives.

Spirion also maintains a Disaster Recovery Plan (DRP) which is designed to protect and guide recovery of the company's information technology equipment. The DRP addresses significant disruption in capabilities and services to Spirion's internal network, as well as technologies that support the Sensitive Data Platform™.

Spirion uses Azure data centers to host the enterprise software solution's production and non-production environments. Azure is contractually obligated to Spirion to maintain security, availability, and confidentiality SOC 2® criteria to satisfy Spirion's contractual obligations. Azure's contractual commitments with Spirion are designed to withstand events that would impact the company's DRP and meet its recovery time objectives.

Security monitoring services are utilized from a sub-service organization to monitor server performance and availability, site availability and security threats. Alerts are generated that invoke the incident response plan.

System Availability

Spirion's Sensitive Data Platform™ runs on Azure clusters across multiple regions for high availability. The clusters are self-healing and any one regional problem does not result in a service disruption. Critical datastores are backed up every six hours. The operations team receives and monitors alerts related to outages or issues within the system. System updates and patches are deployed automatically to one node at a time. Any other image updates provided by Azure are included as part of the change management process to update the application environment.

Spirion corporate systems are also located in Azure with physical systems also onsite in the corporate offices, in a secured room. Corporate systems are responsible for handling access control mechanisms to the systems supporting Spirion's Sensitive Data Platform™. These corporate systems are backed up weekly. The corporate systems are patched every two weeks.

New solutions are reviewed for any security, availability, and confidentiality implications and addressed appropriately through defined testing methodology.

Physical Security

Physical security of customer data and the in-scope enterprise system is the responsibility of Azure. Management obtains and reviews the Azure SOC 2® Type 2 regularly to ensure relevant considerations are being assessed and controls within it align with management's expectations of Azure.

Spirion facility data centers only support internal network systems and computing. Spirion has implemented facility access controls which are documented within the CISP and is the responsibility of Spirion employees. Access to the facility is restricted through a badge access system.

Logical Security

Spirion's local user networks are distinct and isolated from the production network (Azure) in which Spirion applications and customer data are maintained. This segregation of systems access is facilitated through distinct Active Directory domains and firewall rulesets. Administrator-level accounts requires multifactor authentication (MFA) to utilize the accounts. Networks are designed to enforce the least privileges model by maintaining distinct access management technology / solutions.

Changes to the production environment of the Sensitive Data Platform™ application is restricted to members of the operations team supporting the infrastructure and application availability efforts. Role-based access controls (RBAC) are in use to ensure access is granted based on need, as defined by role. Administrator accounts are granted to a limited number of authorized personnel. Further system protections include full disk encryption on production equipment for data at rest.

Spirion management has established and maintains a written process to request new network and facility access or to modify or terminate existing access for employees and contractors. The written process requires separate approval for setting up administrative accounts to any software solution and remote access to the network.

Customers are restricted from accessing other customer data using customer-specific databases, firewall rules and entity-authenticated IDs and passwords. Customers may also elect to restrict access based upon IP whitelisting configurations.

Access control policies do not distinguish between environments. Accordingly, policies and processes are applied uniformly across environments.

Backups

Spirion management has implemented and validated a comprehensive strategy for backup and restoration based on a review of its business requirements.

The operations team uses multi-region security accounts in Azure to backup systems across availability regions. Databases and security keys are backed up every six hours. Production systems run on high availability clusters with self-healing features. Corporate systems are backed up weekly.

Customer backup data can be retained in geographically distinct area from Spirion's primary data center.

Change Management

Application change management is tracked using a change management tool. Developers are required to complete annual job specific training. Daily standups are held to authorize work. An enterprise software package is used for version control and approvals for changes that go into production. Once a software update is deployed to the development environment, automated testing is completed, and the version moves to Quality Assurance (QA). In the QA phase the QA and user acceptance testing (UAT) are completed. The software version then is promoted to a security environment, where application penetration testing is performed prior to releasing a change to production. Application security testing tool(s) runs daily coding security checks on any commits to the security environment. Access to deploy changes to production is restricted to the Cloud Operations team.

Data

Data is assigned a classification in accordance with the data classification criteria defined within the CISP. No confidential customer data is retained outside of the production domain. Spirion takes measures to preserve the confidentiality of data when computer hardware reaches its end of life. Additionally, confidential information is disposed of in a manner that preserves confidentiality.

The CISP stresses the importance of protecting critical business assets with effective security measures including granting limited access requests to only those employees who have a legitimate business need. An Acceptable Use policy is maintained by management and outlines requirements to restrict access to data and the appropriate use of data within the network. Employees are required to acknowledge the security and confidentiality policies, including the Acceptable Use Policy, upon hire and annually thereafter. Contractors, or contracting agencies, sign confidentiality agreements which require contract employees to be trained and employ security standards no less than Spirion's security standards. The CISP and corresponding data security policies are updated no less than annually.

Periodically, and no less than semiannually, the lists of personnel with access to production data are reviewed by management to ensure that only those individuals requiring this level of access have been granted access.

Spirion customer profiles include the name of personnel authorized to contact Spirion for support at the time of handoff. Spirion support personnel are prohibited from providing support to any unauthorized customer personnel without approval from a customer authorized contact.

If an employee is terminated from the organization (voluntarily or involuntarily), the Information Technology Team is promptly notified. On the employee's last day, a member of the Information Technology Team disables the user's network account, disables system application accounts, deactivates the desk phone, and inventories the equipment recovered by Human Resources. Spirion equipment is logged and monitored and any equipment not recovered or received by Human Resources is promptly known and tracked by both Human Resources and the Information Technology Team.

SECTION 4:

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

SERVICE COMMITMENTS AND SYSTEM REQUIREMENTS

Spirion designs its processes and procedures related to Sensitive Data Platform™ system to meet its objectives. Those objectives are based on the service commitments that Spirion makes to user entities, the laws and regulations that govern the provision of Sensitive Data Platform™ and the financial, operational, and compliance requirements that Spirion has established for the services. The Sensitive Data Platform™ of Spirion are subject to the security and privacy requirements of the Health Insurance Portability and Accountability Act Administrative Simplification, as amended, including relevant regulations, as well as state privacy security laws and regulations in the jurisdictions in which Spirion operates.

Security, availability, and commitments to user entities are documented and communicated in Service Level Agreements (SLAs) and other customer agreements, as well as in the description of the service offerings provided online. Security commitments are standardized and include, but are not limited to, the following:

- Security principles within the fundamental design of the system that are designed to permit system users to access the information they need based on their role in the system while restricting them from accessing information not needed for their role.
- Use of encryption technologies to protect customer data both at rest and in transit
- Monthly availability commitments
- Confidential information used solely to exercise its right and perform obligations

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

System descriptions for Spirion's Data Management Services system are available on the customer support portal. Change notes, including changes in control obligations, are also made available on the customer support portal.