Report on SailPoint Technologies, Inc.'s Non-Employee Risk Management Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2023 to October 31, 2024

SOC 3® - SOC for Service Organizations: Trust Services Criteria for General Use Report

Table of Contents

Section 1

Independent Service Auditor’s Report

Independent Service Auditor's Report

To: SailPoint Technologies, Inc. ("SailPoint")

Scope

We have examined SailPoint's accompanying assertion titled "Assertion of SailPoint Technologies, Inc. Management" (assertion) that the controls within SailPoint's Non-Employee Risk Management (system) were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that SailPoint'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 (With Revised Points of Focus—2022)*, in AICPA, *Trust Services Criteria*.

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

SailPoint uses a subservice organization to provide Infrastructure-as-a-Service (IaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SailPoint, to achieve SailPoint's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of SailPoint's controls. Our examination did not include the services provided by the subservice organization, and we have not evaluated the suitability of the design or operating effectiveness of such complementary subservice organization controls.

Service Organization's Responsibilities

SailPoint 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 SailPoint's service commitments and system requirements were achieved. SailPoint has also provided the accompanying assertion about the effectiveness of controls within the system. When preparing its assertion, SailPoint 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 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.

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

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 SailPoint'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 SailPoint'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 were achieved based on the applicable trust services criteria. Also, the projection to the future of any conclusions about the effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within SailPoint's Non-Employee Risk Management were effective throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that SailPoint'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 SailPoint's controls operated effectively throughout that period is fairly stated, in all material respects.

Coalfire Controls LLC

Greenwood Village, Colorado
December 19, 2024

Section 2

Assertion of SailPoint Technologies, Inc. Management

Assertion of SailPoint Technologies, Inc. ("SailPoint") Management

We are responsible for designing, implementing, operating and maintaining effective controls within SailPoint's Non-Employee Risk Management (system) throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that SailPoint'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 (With Revised Points of Focus—2022),* in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented in attachment A and identifies the aspects of the system covered by our assertion.

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

SailPoint uses a subservice organization for Infrastructure-as-a-Service (IaaS) services. The description of the boundaries of the system indicates that complementary subservice organization controls that are suitably designed and operating effectively are necessary, along with controls at SailPoint, to achieve SailPoint's service commitments and system requirements based on the applicable trust services criteria. The description of the boundaries of the system presents the types of complementary subservice organization controls assumed in the design of SailPoint's controls. The description of the boundaries of the system does not disclose the actual controls at the subservice organization.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2023 to October 31, 2024, to provide reasonable assurance that SailPoint'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 SailPoint's controls operated effectively throughout that period. SailPoint'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 attachment B.

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 November 1, 2023 to October 31, 2024, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the applicable trust services criteria.

SailPoint Technologies, Inc.

Attachment A

SailPoint Technologies, Inc.’s Description of the Boundaries of Its Non-Employee Risk Management

Overview of the Company

SailPoint Technologies, Inc. (“SailPoint” or the “Company”) provides identity security solutions to clients in a variety of industries, including energy, financial services, healthcare, insurance, and the public sector. Overall, these solutions are intended to help clients better manage and evaluate access to their information technology (IT) systems to ensure that access is appropriate based on users’ roles within the environments. Elements of these solutions include the following:

- Compliance Management – Intended to streamline the execution of compliance controls and improve audit performance through automated access certifications, policy management, and audit reporting.
- Provisioning – Intended to speed the delivery of access to the business while reducing costs and tightening security with self-service access requests, approvals, automated provisioning, and full identity lifecycle management.
- Password Management – Intended to promote user productivity while reducing IT and help desk costs with intuitive self-service password management.
- Artificial Intelligence (AI) Services – Highlights access risks across the entire enterprise, provides insights to help user entities make effective business decisions, and creates access models that ensure that appropriate access is assigned to users.

Type of Services Provided

The core of SailPoint solutions is the utilization of the following applications:

- **Identity Security Cloud** (formerly referenced as “SaaS Service,” which included IdentityNow, AI services, and Cloud Infrastructure Entitlement Management): SailPoint’s software-as-a-service (SaaS) identity security offering provides customers a suite of integrated solutions for intelligently managing a range of identity needs across access modeling, lifecycle management, compliance management, analytics, password management, and Cloud Infrastructure Entitlement Management. It can be used in conjunction with SailPoint’s other SaaS services as listed below (Cloud Access Management, Non-Employee Risk Management, Access Risk Management, SaaS Management, and Data Access Security).
- **Additional SailPoint SaaS services**:
  - Cloud Access Management: Uses AI and machine learning (ML) to automatically learn, monitor, and help provide secure access to cloud infrastructure.
  - Non-Employee Risk Management: Governs the lifecycle of non-employee populations through the onboarding, provisioning, and governing of access for third parties that require access to customers’ IT ecosystem.
  - Access Risk Management: Automates Systems Applications and Products (SAP) access controls to include segregation of duties, sensitive access monitoring, and emergency access management.
  - SaaS Management: Provides visibility across internal software subscriptions to manage unused licenses, SaaS spending, usage, and security and compliance data.

  - Data Access Security: Provides Data Access Governance solutions to help organizations discover, govern and secure identity's real-time access to sensitive data with an emphasis on unstructured data. The solution is designed to do the following: secure critical unstructured data through data discovery, data classification and cataloging sensitive and regulated data, understand access patterns to data through permissions analysis ensuring access to such assets is appropriate based on users' role and attributes within the environment and provide forensics capabilities and surface the effective access that entitlements and roles grant to that critical data.
- **IdentityIQ**: SailPoint's identity governance product that can be delivered from the cloud or on premises to enable organizations to safely accelerate digital transformation. IdentityIQ's Compliance Manager, Lifecycle Manager, and File Access Manager modules govern access to applications, data, and multi-cloud platforms. It can be used in conjunction with the Company's Identity Service Cloud, including Access Insights, Recommendation Engine, Access Modeling, and Cloud Access Management.

The boundaries of the system in this section details Non-Employee Risk Management. Any other SailPoint products or services are not within the scope of this report, including Identity Security Cloud, IdentityIQ, IdentityIQ Cloud Managed Service, SaaS Management and Access Risk Management.

The Boundaries of the System Used to Provide the Services

The boundaries of the system are the specific aspects of SailPoint's infrastructure, software, people, procedures, and data necessary to provide its services and that directly support the services provided to customers. Any infrastructure, software, people, procedures, and data that indirectly support the services provided to customers are not included within the boundaries of Non-Employee Risk Management.

The components that directly support the services provided to customers are described in the subsections below.

Infrastructure

The Company utilizes Amazon Web Services (AWS) to provide the resources to host Non-Employee Risk Management. SailPoint leverages the experience and resources of AWS to enable the Company to scale quickly and securely as necessary to meet current and future demand. However, the Company is responsible for designing and configuring Non-Employee Risk Management's architecture within AWS to ensure that availability, security, and resiliency requirements are met.

SailPoint relies on AWS for the following:

- Providing physical and environmental safeguards around the physical servers and related infrastructure.
- Operating, managing, and controlling the components from the virtualization layer down to the physical security of the facilities in which the services operate.
- Performing user physical access administration controls related to the Non-Employee Risk Management's production environments.
- Performing backups of Non-Employee Risk Management's databases (which include client data) as directed by SailPoint.

- Maintaining a web portal and application programming interface (API) used by SailPoint to manage the configuration of its cloud environment, including management of access privileges.
- Providing other services documented in AWS' Shared Responsibility: Model: https://aws.amazon.com/compliance/shared-responsibility-model/.

Software

Non-Employee Risk Management is a SaaS service that is comprised of the following:

- Non-Employee Lifecycle – Workflow systems to enable the collection, review, approval, and management of the non-employee identities that require access to an organization's network.
- Non-Employee Collaboration Portal – Secure delegation of non-employee identity management processes and tasks to external business partners.
- Customizable Forms and Views – Configuration of the collection and management of non-employee identity data to meet an organization's business processes and use cases.
- Risk Scoring – Attribute- and relationship-based risk scores for non-employees and their related business partners.
- Reporting – Easy CSV export of configurable sets of non-employee data.
- Auditing – Complete history of change events for both non-employee data and application configuration settings.

To manage the software development process, the Company uses a wide array of software tools, which include the following:

- Agile application lifecycle management tools are used to document, track, and manage defects and application enhancements.
- A source code management repository is used to store and track versions of production source code.
- A source code control solution and repository management tool are used to manage code merge requests.
- Security groups are configured and utilized to prevent unauthorized network access.
- Security testing tools are used to ensure that software is secure before it is deployed.
- Automated deployment tools are used to deploy builds.
- A log management tool is utilized to identify indicators of malicious activity, and the logs are sent to a security operations center.
- Host- and network-based intrusion detection systems (IDSs) are used to monitor the infrastructure.

People

The Company develops, manages, and secures Non-Employee Risk Management via separate departments, including Engineering, DevOps, Customer Success, Cybersecurity, IT, and Human Resources (HR). The responsibilities of these departments are defined below in the Organizational Structure section.

Procedures

Formal policies exist that describe the software development lifecycle (SDLC), logical security requirements, network and system hardening standards, change management, incident management, data classification, and HR procedures. All personnel are expected to adhere to the Company's policies. The policies are located on the Company's intranet and are updated at least annually. Changes to these policies are communicated to all Company personnel in a timely manner.

Data

Client data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts. This client data is managed and stored within Non-Employee Risk Management. Each client determines and is responsible for the data uploaded within their Non-Employee Risk Management production environments.

Customer data is managed, processed, and stored in accordance with relevant data protection and other regulations and with specific requirements formally established in client contracts.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Encryption is enabled for data stores housing sensitive customer data.

Complementary User Entity Controls (CUECs)

The Company's controls related to Non-Employee Risk Management cover only a portion of overall internal control for each user entity of Non-Employee Risk Management. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by the Company. Therefore, each user entity's internal control should be evaluated in conjunction with the Company's controls, taking into account the related CUECs identified for the specific criterion. In order for user entities to rely on the controls reported herein, each user entity must evaluate its own internal control to determine whether the identified CUECs have been implemented and are operating effectively.

The CUECs presented should not be regarded as a comprehensive list of all controls that should be employed by user entities. Management of user entities is responsible for the following:

Criteria	Complementary User Entity Controls
CC2.1	• User entities have policies and procedures to report any material changes to their overall control environment that may adversely affect services being performed by the Company according to contractually specified time frames. • Controls to provide reasonable assurance that the Company is notified of changes in: – User entity vendor security requirements – The authorized users list
CC2.3	• It is the responsibility of the user entity to have policies and procedures to: – Inform their employees and users that their information or data is being used and stored by the Company. – Determine how to file inquiries, complaints, and disputes to be passed on to the Company. • User entities have policies and procedures for communicating support requests to the Company in a timely manner. • User entities have policies and procedures for ensuring that system administrators and other relevant users are enrolled to receive updates through the Company's website.

Criteria	Complementary User Entity Controls
CC6.1	• Controls to provide reasonable assurance that policies and procedures are deployed over user IDs and passwords that are used to access services provided by the Company. • Default application administrator passwords should be changed upon initial setup of the application. • Segregation of duties between user entity employees is maintained, and the concept of least privilege is maintained.
CC6.1 CC6.2	• User entities grant access to the Company's system to authorized and trained personnel. • Controls should be established to ensure that appropriate and authorized access to Non-Employee Risk Management has been granted.
CC6.2 CC6.3	• Controls should determine that authorized users and their associated access privileges are reviewed periodically. • User entities should ensure timely removal of user accounts for any users that have been terminated and were previously involved in any material functions or activities associated with Non-Employee Risk Management.
CC6.4 CC6.5 CC7.2 A1.2	• User entities deploy physical security and environmental controls for all devices and access points residing at their operational facilities, including remote employees or at-home agents for which the user entity allows connectivity.

Subservice Organization and Complementary Subservice Organization Controls (CSOCs)

The Company uses AWS as a subservice organization for IaaS. The Company's controls related to Non-Employee Risk Management cover only a portion of the overall internal control for each user entity of Non-Employee Risk Management.

Although the subservice organization has been carved out for the purposes of this report, certain service commitments, system requirements, and applicable criteria are intended to be met by controls at the subservice organization. CSOCs are expected to be in place at AWS related to physical security and environmental protection, as well as backup, recovery, and redundancy controls related to availability. AWS' physical security controls should mitigate the risk of unauthorized access to the hosting facilities. AWS' environmental protection controls should mitigate the risk of fires, power loss, climate, and temperature variabilities.

Company management receives and reviews the AWS SOC report annually. In addition, through its operational activities, Company management monitors the services performed by AWS to determine whether operations and controls expected to be implemented are functioning effectively. Management also communicates with the subservice organization to monitor compliance with the service agreement, stay informed of changes planned at the hosting facility, and relay any issues or concerns to AWS management.

It is not feasible for the service commitments, system requirements, and applicable criteria related to Non-Employee Risk Management to be achieved solely by the Company. Therefore, each user entity's internal control must be evaluated in conjunction with the Company's controls, taking into account the related CSOCs expected to be implemented at AWS as described below.

Criteria	Complementary Subservice Organization Controls
CC6.1	• AWS is responsible for ensuring that all data in its control is encrypted at rest.
CC6.4	• AWS is responsible for restricting data center access to authorized personnel. • AWS is responsible for the 24/7 monitoring of data centers by closed circuit cameras and security personnel.
CC6.5 CC6.7	• AWS is responsible for securely decommissioning and physically destroying production assets in its control.
CC6.6 CC6.8 CC7.2 CC7.3 CC8.1	• AWS is responsible for the patching of infrastructure supporting the service as a part of routine maintenance and as a result of identified vulnerabilities to help ensure that servers supporting the service are hardened against security threats.
CC7.2 A1.2	• AWS is responsible for the installation of fire suppression and detection and environmental monitoring systems at the data centers. • AWS is responsible for protecting data centers against a disruption in power supply to the processing environment by an uninterruptible power supply (UPS). • AWS is responsible for overseeing the regular maintenance of environmental protections at the data centers.
A1.2	• AWS is responsible for performing backups of the databases (which include client data) as directed by SailPoint.

Attachment B

Principal Service Commitments and System Requirements

Principal Service Commitments and System Requirements

Commitments are declarations made by management to customers regarding the performance of Non-Employee Risk Management. Commitments are communicated in the SailPoint Framework Customer Agreement and the Support Policy. The Company's commitments include the following:

- SailPoint will maintain administrative and technical safeguards designed to protect the security and confidentiality of customer data, including measures designed to prevent unauthorized access, use, modification, or disclosure of customer data.
- SailPoint will only use customer confidential information to perform agreed-upon obligations and will not disclose customer confidential information to any third party other than contractors who are subject to confidentiality agreements.
- SailPoint will provide 99.9% system availability during each calendar month.
- SailPoint will use the same degree of care to protect customer confidential information that it uses to protect its own confidential information of like nature, but no less than a reasonable degree of care.
- SailPoint will provide premium support and maintenance services that include telephone and electronic support, bug fixes and code corrections, as well as updates and enhancements.

The Company provides external users with guidelines and technical support resources related to system operations on a website made available to customers. The Company provides an external-facing support system and contact information to allow users to report system information on failures, incidents, concerns, and other complaints to the appropriate personnel. The Company notifies customers of critical changes that may affect their processing.

System requirements are specifications regarding how Non-Employee Risk Management should function to meet the Company's commitments to customers. Requirements are specified in the Company's policies and procedures, which are available to all employees. The Company's system requirements include the following:

- Employee provisioning and deprovisioning standards
- Logical access controls such as use of user IDs and passwords to access systems
- Risk assessment standards
- Data encryption at rest and in transit
- Incident response policies, procedures, and plan
- Anti-malware technology
- Backup and recovery standards
- Business continuity/disaster recovery (BC/DR) plan
- Change management controls
- Monitoring controls
- Data classification policies and procedures
- Data retention and disposal policies and procedures