COALFIRE
CONTROLS

Report on SailPoint Technologies, Inc.'s IdentityIQ Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2022 to October 31, 2023

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

SailPoint®

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 IdentityIQ (system) were effective throughout the period November 1, 2022 to October 31, 2023, 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)* (2017 TSC).

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.

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 service 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 IdentityIQ were effective throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the applicable trust services criteria if 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 27, 2023

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 IdentityIQ (system) throughout the period November 1, 2022 to October 31, 2023, 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)* (2017 TSC). 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.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period November 1, 2022 to October 31, 2023, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the applicable trust services criteria if 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, 2022 to October 31, 2023, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the applicable trust services criteria.

SailPoint Technologies, Inc.

![COALFIRE CONTROLS]

Attachment A

SailPoint Technologies, Inc.'s Description of the Boundaries of Its IdentityIQ

Overview of the Company

SailPoint Technologies, Inc. ("SailPoint" or the "Company") provides identity governance 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 improves 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:

- **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 software-as-a-service (SaaS) Service, including Access Insights, Recommendation Engine, Access Modeling, and Cloud Access Management.

- **IdentityNow:** SailPoint's SaaS identity governance product. It provides customers with a set of integrated solutions for managing a range of identity needs across access requests, provisioning, password management, access certifications, and separation of duties. It can be used in conjunction with SailPoint's other SaaS Service, including Access Insights, Recommendation Engine, Access Modeling, Cloud Access Management, Cloud Infrastructure Entitlement Management and Non-Employee Risk Management.

- **Additional SailPoint SaaS services:**
  - SailPoint AI services:
    - Access Insights: Helps turn identity data collected into actionable insights, including automated outlier detection.
    - Recommendation Engine: Uses AI, machine learning (ML), peer group analysis, identity attributes, and access activity to help customers decide whether access should be granted to or removed from users.
    - Access Modeling: Uses AI and ML to suggest roles based on similar access between users and is intended to give customers insights to confirm the correct access for each role.

- Cloud Access Management: Uses AI and ML to automatically learn, monitor, and help provide secure access to cloud infrastructure.
- SaaS Management: Provides visibility across internal software subscriptions to manage unused licenses, SaaS spending, usage, and security and compliance data.
- Access Risk Management: Automates SAP access controls to include segregation of duties, sensitive access monitoring, and emergency access management.
- 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 our customers' IT ecosystem.

The boundaries of the system in this section details IdentityIQ, delivered on-premises. Any other SailPoint products or services are not within the scope of this report, including IdentityIQ Cloud Managed Service, SaaS Service (IdentityNow, AI services, Cloud Access Management and Cloud Infrastructure Entitlement Management), SaaS Management, Access Risk Management, and Non-Employee Risk Management. This report does not include additional support related to change management of IdentityIQ once installed by a user entity.

The Boundaries of the System Used to Provide the Services

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

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

Software

IdentityIQ is a product comprised of the following:

- Access Requests and Approvals – Allows users to request and fulfill application and data access needs while adhering to corporate governance controls.
- Access Certification – Automates the process of certifying user access rights across the organization by initiating campaigns for managers to review and approve or revoke access.
- User Provisioning – Fully automates the user provisioning service to streamline creating, changing, and revoking user access based on user life cycle events and role definitions.
- Policy Management – Implements, enforces, and monitors access permissions and activity to reduce the risk of fraud or compliance violations.
- Password Management – Manages user passwords across cloud and on-premises applications across desktop browsers or mobile devices.

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

- Agile application life cycle 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.
- Firewalls are configured and utilized to prevent unauthorized 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 trends that may impact the Company's security objectives.
- Host and network-based intrusion detection systems (IDSs) are used to monitor the infrastructure.

People

The Company develops, manages, and secures IdentityIQ via separate departments, including Engineering, 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 Life Cycle (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

There is no client data used in the development or testing of IdentityIQ.

Complementary User Entity Controls (CUECs)

The Company's controls related to IdentityIQ cover only a portion of overall internal control for each user entity of IdentityIQ. 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
CC2.3	- 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	• Segregation of duties between user entity employees is maintained, and the concept of least privilege is maintained. • 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.
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 IdentityIQ 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 IdentityIQ.
CC6.4 CC6.5 CC7.2 A1.2	• User entities have adequate 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.
CC6.6 CC6.7	• Secure data transmission protocols are used to encrypt confidential and sensitive data when transmitted over public networks.
CC6.6 CC6.8 CC7.2 CC7.3 CC8.1	• Infrastructure supporting the service is patched 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	• An infrastructure monitoring tool is utilized to monitor system or infrastructure availability and performance and generates alerts when specific, predefined thresholds are met.
A1.1	• User entities evaluate system capacity and implement changes to ensure the processing capacity can meet demand.
A1.2	• User entities document formal procedures that outline the process to back up and recover customer data. • User entities configure backups for data stores housing sensitive data.
C1.2	• User entities purge or remove confidential information from the environment.

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 IdentityIQ. Commitments are communicated in the SailPoint Framework Customer Agreement and Support Policy. The Company's commitments include the following:

- 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.

System requirements are specifications regarding how IdentityIQ 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 the use of user IDs and passwords to access systems
- Risk assessment standards
- Incident response policies, procedures, and plan
- Business continuity/disaster recovery (BC/DR) plan
- Change management controls
- Monitoring controls
- Data classification policies and procedures