Report on SailPoint Technologies, Inc.'s IdentityNow and AI products Relevant to Security, Availability, and Confidentiality Throughout the Period November 1, 2019 to October 31, 2020

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

COALFIRE CONTROLS

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 the IdentityNow and AI products (system) were effective throughout the period November 1, 2019 to October 31, 2020, 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* (AICPA, *Trust Services Criteria*).

The description of the boundaries of the system indicates that certain 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 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 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 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 the IdentityNow and AI products were effective throughout the period November 1, 2019 to October 31, 2020, 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

Westminster, Colorado
December 23, 2020

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 the IdentityNow and AI products (system) throughout the period November 1, 2019 to October 31, 2020, to provide reasonable assurance that SailPoint'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 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, 2019 to October 31, 2020, 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* (AICPA, *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, 2019 to October 31, 2020, 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 IDENTITYNOW AND AI PRODUCTS

TYPE OF SERVICES PROVIDED

SailPoint Technologies, Inc. (together with its affiliates "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 help streamline the execution of compliance controls and improve audit performance through automated access certifications, policy management, and audit reporting.
- Provisioning – Intended to help speed the delivery of access to businesses while reducing costs and tightening security with self-service access requests and automated provisioning.
- Password Management – Intended to promote user productivity while reducing IT and help desk costs with intuitive self-service password management.
- Identity Intelligence – Helps centralize visibility into access risks across an organization and provide insights to assist with business decision making.

SailPoint's product portfolio consists of the following:

- **IdentityNow**: SailPoint's software-as-a-service (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 products, including Access Insights, Recommendation Engine, Access Modeling, Cloud Access Management, and Workload Privilege Management.
- **Additional SailPoint SaaS products**
  - SailPoint AI products (formally known as IdentityAI)
    - Access Insights: Helps turn identity data collected into actionable insights.
    - 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.
  - Workload Privilege Management: Automates the creation and rotation of credentials, keys, passwords and records, and logs activity whenever privileged tasks are performed for security and audit purposes.
- **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 our SaaS products, including Access Insights, Recommendation Engine, Access Modeling, Cloud Access Management and Workload Privilege Management.

The description of the boundaries of the system in this section of the report details IdentityNow and AI products. Any other SailPoint products or services are not within the scope of this report, including IdentityIQ Cloud Managed Service, Cloud Access Management, and Workload Privilege 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 the system.

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 IdentityNow and AI products. 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 the IdentityNow and AI products' 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 host operating system (OS) and virtualization layer down to the physical security of the facilities in which the services operate.
- Performing user physical access administration related to the IdentityNow and AI products' production environments (as directed by SailPoint).
- Performing backups of the IdentityNow and AI products' databases (which include client data) as directed by SailPoint.
- Maintaining a web portal that is used by SailPoint to manage the configuration of its cloud environment, including management of access privileges.

SOFTWARE

IdentityNow is a SaaS solution that is comprised of the following products:

- Password Management – Enables users to manage password changes and resets across on-premises and cloud applications without having to call the help desk.
- Access Certification – Automates the process of certifying user access rights across an organization by initiating campaigns for managers to review and approve or revoke access.
- Provisioning – Fully automates the user provisioning service to help streamline creating, changing, and revoking user access based on user life cycle events and role definitions.
- Access Request – Provides a self-service platform for requesting and approving access to applications.
- Separation of Duties – Fully automates the process of defining and executing policies to help ensure that employees do not possess access that is in violation of compliance directives that an organization prescribes to.

SailPoint's AI solutions are SaaS products that are comprised of the following:

- Access Insights – Uses a wide variety of identity-related data to help teams examine their governance past, evaluate their governance present, and plan for their governance future.
- Recommendation Engine – Provides recommendations to approvers/reviewers, improving the efficiency and effectiveness of governance and compliance actions. Recommendation Engine can also be used to fully automate the decision-making process for certifications.
- Access Modeling – Intended to enable identity professionals to maintain access policies or roles efficiently and accurately for an organization. Access Modeling utilizes AI and identity data to help proactively define and suggest access models in an effort to enable and secure employees' access within an organization.

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 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.
- Intrusion detection systems (IDSs) are used to monitor the Company's network.

PEOPLE

The Company develops, manages, and secures the IdentityNow and AI products via separate departments, including Engineering, SaaS DevOps, Customer Success and Support, Security, 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), physical and 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 IdentityNow and AI products. Each client determines and is responsible for the data uploaded within their IdentityNow and AI production environments.

AI product data is additionally managed and stored in Curation, a dedicated data storage space, and is under the same level of scrutiny and controls as the production environment. The purpose of the data in this environment is to support debugging for any issues that may arise in the AI and Machine Learning pipeline, ML algorithm design and development, and service engagements.

The Company has deployed secure methods and protocols for transmission of confidential or sensitive information over public networks. Databases housing sensitive customer data are encrypted at rest.

COMPLEMENTARY USER ENTITY CONTROLS (CUECS)

SailPoint's controls related to IdentityNow and AI products cover only a portion of overall internal control for each user entity of IdentityNow and AI products. It is not feasible for the service commitments, system requirements, and applicable criteria related to the system to be achieved solely by SailPoint. Therefore, each user entity's internal control should be evaluated in conjunction with SailPoint's controls considering the related CUECs identified for the specific criterion. 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 (CUECs)
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.
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	• Controls should be established to ensure that appropriate and authorized access to IdentityNow and AI products have 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 IdentityNow and AI products.
CC6.4 CC6.5 CC7.2 A1.2	• User entities have adequate physical security and environmental controls of 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)

SailPoint uses AWS as a subservice organization for infrastructure-as-a-service (IaaS). SailPoint's controls related to IdentityNow and AI products cover only a portion of the overall internal control for each user entity of IdentityNow and AI products.

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 mitigate the risk of fires, power loss, climate, and temperature variabilities.

SailPoint management receives and reviews the AWS SOC report at least annually. In addition, through its operational activities, SailPoint management monitors the services performed by AWS to determine whether operations and controls expected to be implemented at the subservice organization 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 the IdentityNow and AI products to be achieved solely by SailPoint. Therefore, each user entity's internal control must be evaluated in conjunction with SailPoint's controls considering the related CSOCs expected to be implemented at the subservice organization as described below.

Criteria	Complementary Subservice Organization Controls (CSOCs)
CC6.1	• AWS is responsible for ensuring all data 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.
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 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 IdentityNow and AI products. Commitments are communicated in SaaS agreements, service level agreements, or other written documentation. 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 personal data.
- SailPoint will only use confidential information to perform agreed-upon obligations and will not disclose 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 shall use the same degree of care to protect 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 Identity as a Service Support and Maintenance Services including telephone and electronic support, bug fixes and code corrections, changes to the SaaS service and customer contracts with access to support services.

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 IdentityNow and AI products 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
- 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