A-LIGN

SailPoint Technologies, Inc.

Type 2 SOC 3

2023

SailPoint

A-LIGN.COM

SOC 3 FOR SERVICE ORGANIZATIONS REPORT

April 1, 2022 to March 31, 2023

Table of Contents

SECTION 1

ASSERTION OF SAILPOINT TECHNOLOGIES, INC. MANAGEMENT

ASSERTION OF SAILPOINT TECHNOLOGIES, INC. MANAGEMENT

April 19, 2023

We are responsible for designing, implementing, operating, and maintaining effective controls within SailPoint Technologies, Inc.'s ('SailPoint' or 'the Company') Non-Employee Risk Management Services throughout the period April 1, 2022 to March 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 and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA, *Trust Services Criteria*. Our description of the boundaries of the system is presented below in "SailPoint Technologies, Inc.'s Description of Its Non-Employee Risk Management Services throughout the period April 1, 2022 to March 31, 2023" and identifies the aspects of the system covered by our assertion.

We have performed an evaluation of the effectiveness of the controls within the system throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the trust services criteria. 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 "SailPoint Technologies, Inc.'s Description of Its Non-Employee Risk Management Services throughout the period April 1, 2022 to March 31, 2023".

SailPoint uses Amazon Web Services ('AWS' or 'subservice organization') to provide cloud hosting services. The description 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 presents SailPoint's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SailPoint's controls. The description does not disclose the actual controls at the subservice organization.

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

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 April 1, 2022 to March 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 subservice organization controls and complementary user entity controls assumed in the design of SailPoint's controls operated effectively throughout that period.

rex booth

Rex Booth
Chief Information Security Officer
SailPoint Technologies, Inc.

SECTION 2

INDEPENDENT SERVICE AUDITOR’S REPORT

INDEPENDENT SERVICE AUDITOR'S REPORT

To SailPoint Technologies, Inc.:

Scope

We have examined SailPoint Technologies, Inc.'s ('SailPoint' or 'the Company') accompanying assertion titled "Assertion of SailPoint Technologies, Inc. Management" (assertion) that the controls within SailPoint's Non-Employee Risk Management Services were effective throughout the period April 1, 2022 to March 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 and Confidentiality (applicable trust services criteria) set forth in TSP section 100, *2017 Trust Services Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*, in AICPA *Trust Services Criteria*.

SailPoint uses AWS to provide cloud hosting services. The description 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 presents SailPoint's controls, the applicable trust services criteria, and the types of complementary subservice organization controls assumed in the design of SailPoint's controls. The description does not disclose the actual controls at the subservice organization. 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.

The description 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 presents SailPoint's controls, the applicable trust services criteria, and 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 (SailPoint 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 AICPA. 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 the description is not presented in accordance with the description criteria and that controls were not suitably designed or did not operate effectively
- Performing procedures to obtain evidence about whether controls stated in the description were suitably designed to provide reasonable assurance that the service organization achieved its service commitments and system requirements based on the applicable trust services criteria

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

Independence and Ethical Responsibilities

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

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 conclusions about the suitability of the design and operating effectiveness of controls is subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion

In our opinion, management's assertion that the controls within SailPoint's Non-Employee Risk Management Services were suitably designed and operating effectively throughout the period April 1, 2022 to March 31, 2023, to provide reasonable assurance that SailPoint's service commitments and system requirements were achieved based on the applicable trust services criteria is fairly stated, in all material respects, if complementary subservice organization controls and complementary user entity controls assumed in the design of SailPoint's controls operated effectively throughout that period.

The SOC logo for Service Organizations on SailPoint's website constitutes a symbolic representation of the contents of this report and is not intended, nor should it be construed, to provide any additional assurance.

Restricted Use

This report, is intended solely for the information and use of SailPoint, user entities of SailPoint's Non-Employee Risk Management Services during some or all of the period April 1, 2022 to March 31, 2023, business partners of SailPoint subject to risks arising from interactions with the Non-Employee Risk Management Services, and those who have sufficient knowledge and understanding of the complementary subservice organization controls and complementary user entity controls and how those controls interact with the controls at the service organization to achieve the service organization's service commitments and system requirements.

This report is not intended to be, and should not be, used by anyone other than these specified parties.

A-LIGN ASSURANCE

Tampa, Florida
April 19, 2023

SECTION 3

SAILPOINT TECHNOLOGIES, INC.'S DESCRIPTION OF ITS NON-EMPLOYEE RISK MANAGEMENT SERVICES THROUGHOUT THE PERIOD APRIL 1, 2022 TO MARCH 31, 2023

OVERVIEW OF OPERATIONS

Company Background

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.

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

- 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 role design, access requests, provisioning, password management, access certifications, and separation of duties. It can be used in conjunction with SailPoint’s other SaaS services, including Access Insights, Recommendation Engine, Access Modeling, Cloud Access Management, SaaS Management and Access 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 and other leading ERP system access controls to include separation of duties, sensitive access monitoring, and emergency access management.
    - Non-Employee Risk Management: Governs the lifecycle of non-employee populations through the safe onboarding, provisioning, and governing of access for 3rd parties that require access to our customers’ IT ecosystem.
- 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 Company’s SaaS Services, including Access Insights, Recommendation Engine, Access Modeling, and Cloud Access Management.

Description of Services Provided

The Non-Employee Risk Management Services enables organizations to collect third-party, non-employee data in a collaborative and continuous manner, from both internal and external sources, throughout the lifecycle of the third-party. Because third-parties are widely acknowledged by security professionals as high risk, the Non-Employee Risk Management Services applies special consideration at the individual identity level when providing insider access to facilities, systems, and data. The Non-Employee Risk Management Services functions as an identity authority for third-party individual user data that organizations leverage to automate key identity processes, improve operational efficiency and accuracy in onboarding, streamline compliance audits, provide identity verification, and deprovision access in a timely manner.

Automated Design

The Non-Employee Risk Management Services provides users to design business processes and workflows with a drag and drop interface, allowing users to build workflows without code. Point and click interface allow admins to easily configure / manage the solution, without expensive customizations or the need to constantly engage professional services to make changes. Admins can easily create and modify workflows, attributes, views, forms, and built-in actions as building blocks.

Extensible Integration

The Non-Employee Risk Management Services enables integration with customers' existing authentication mechanisms using Lightweight Directory Access Protocol (LDAP) and Security Assertion Markup Language (SAML). While an LDAP directory is included out of the box, these solutions easily attach to Active Directory (AD). External integrations can be included as workflow actions to allow for real time data synchronization using Representational State Transfer (REST) and Simple Object Access Protocol (SOAP) Application Programming Interfaces (API). The Non-Employee Risk Management Services offers several out of the box integrations that allow for easy set up to an HR System, Identity and Access Management (IAM) or even a ticketing system.

User Interaction

The Non-Employee Risk Management Services provides multiple ways for customers to interact with workflow allowing many contributors to collaborate in the management of the full non-employee lifecycle. Non-employees can provide and maintain their own identity data via the self-service portals allowing third-parties to self-register and provide information.

Reporting

The Non-Employee Risk Management provides a central repository of customer, employee, non-employee, and third-party data allowing customers to have a 360 view of their internal and external resources.

Licensing

Non-Employee Risk Management offers a hosted solution within the AWS environment and software licensing on a subscription basis.

Principal Service Commitments and System Requirements

SailPoint designs its processes and procedures related to its software-as-a-service solutions to meet its objectives. Those objectives are based on the service commitments that SailPoint makes to user entities, the laws and regulations that govern the provision of the solutions and the financial, operational and compliance requirements that SailPoint has established for the solutions.

The organization maintains contractual requirements with each of its third-parties. SailPoint maintains master agreements and service level agreements for each customer. Customers must enter into an agreement with SailPoint in order to access the solutions and services. Each customer agreement includes information about payment terms, termination of service, confidentiality, representations and warranties, limitations of liability, indemnifications, and other pertinent subjects.

Security and availability commitments are standardized and include:

- Customer personal data is processed in accordance with application data protection and privacy laws
- Customer sensitive data is retained in confidence
- SailPoint will take reasonable precautions to protect against threats introduced from software virus, trojan horse or similar harmful code
- System access is implemented according to need-to-know, least privilege and separation of duties
- SailPoint uses encryption algorithms, consistent with practices adopted and implemented by SaaS providers, designed to limit unauthorized access to client data

System requirements define how the Non-Employee Risk Management Services should function to meet their commitments to customers. Requirements are specified in SailPoint's policies and procedures which are available to employees. Non-Employee Risk Management system requirements include the following:

- Monitoring controls
- Change management controls
- Provisioning and de-provisioning standards
- Risk and control assessment requirements
- Secure application development

SailPoint maintains an Information Security Policy which addresses the confidentiality, integrity, and availability of SailPoint assets and safeguarding of Sensitive data.

Components of the System

Infrastructure

The Non-Employee Risk Management Services is currently offered as a multi-tenant SaaS solution, hosted in AWS Elastic Container Service (ECS) Fargate. The Non-Employee Risk Management Services make extensive use of the AWS technologies to provide services including, but not limited to:

- Simple Storage Service (S3)
- Relational Database Service (RDS)
- ECS Fargate
- ECS on Elastic Compute Cloud (EC2)
- Elastic Container Registry (ECR)
- Virtual Private Cloud (VPC)
- IAM
- AWS Systems Manager (SSM)
- Elastic Load Balancing (ELB)
- Route 53
- AWS Shield
- Elasticache
- CloudWatch
- CodeCommit
- AWS Web Application Firewall (WAF)
- WatchTower
- ClientVPN
- Various other Amazon provided network technologies

Software

SailPoint's product teams, including developers and testers work together to design, develop, and test the solutions across development and testing environments. Software is developed in accordance with product team coding standards. Change control procedures are used to govern application development changes. System changes are tracked in a commercial tracking software. Each change must be requested, documented, reviewed, approved, and closed. Version control software is used to provide version control and limit access to SailPoint's application code. Code is reviewed and approved for each submission prior to check-in. Scans are conducted pre-release and performed to test the products for vulnerabilities. The customer support ticketing system is used to track client issues and help ensure proper resolution.

Primary software used to provide SailPoint's Non-Employee Risk Management Services includes the following:

Primary Software	
Software	**Purpose**
GitHub	Centralized source control
Zendesk	Client support tickets
Lifecycle	Change Management, Access Request, Incident Reporting, Various Communication
AD	Directory Service for Windows Domain Networks
ClientVPN	Virtual Private Network (VPN) to customer environments

People

SailPoint has established a framework that supports relevant aspects of information security with policies and standards. Led by the Chief Executive Officer (CEO), the framework includes an organizational structure for security and availability, defined by roles and responsibilities for supporting the information security management system.

SailPoint's staff is organized in the following functional areas:

- Senior Management Team: consists of the CEO and other Executive and senior staff. Responsible for overseeing company-wide activities, establishing, and accomplishing goals and overseeing objectives
- Security Administrators: responsible for managing, monitoring, and supporting operations and security
- Compliance: responsible for ensuring that SailPoint is conducting its business in full compliance with professional standards, accepted business practices and internal policies and procedures
- Software development: responsible for the development of new features and addressing application defects
- Quality Assurance: responsible for testing the product
- Professional Services: responsible for providing timely technical services and expertise to customers
- Product Management: responsible for the product planning and execution throughout the Product Lifecycle, including gathering and prioritizing product and customer requirements, defining the product vision, and working closely with engineering, sales, marketing, and support to ensure revenue and customer satisfaction
- Sales: responsible for sales and the development and maintenance of partnerships
- Customer Support: responsible for providing timely technical support to customers

Data

SailPoint manages sensitive data within the system in order to maintain internal control. SailPoint treats customer data within the hosted environment as confidential and does not use or share the information collected.

SailPoint retains customer data based on a defined schedule in accordance with language in the customer's Master Services Agreement. SailPoint has defined retention schedules addressing storage requirements for email, customer data, customer backups and audit logs.

Sensitive data in transit is always encrypted using Transport Layer Security (TLS), using a certificate from a well-known provider. Data is stored in AWS. Customer's encryption requirements are defined in the customer's Master Services Agreement. Encryption for data at rest is always encrypted using Advanced Encryption Standard (AES)-256.

Processes, Policies and Procedures

Formal IT policies and procedures exist that describe physical security, logical access, computer operations, change control, and data communication standards. The teams are expected to adhere to SailPoint policies and procedures that define how services should be delivered. These are located on SailPoint's Policy Portal and can be accessed by any Company team member.

<u>Physical Security</u>

SailPoint leverages AWS-owned facilities that restrict unauthorized access and are protected via various physical perimeter and secured entry points. AWS implements controls, builds automated systems, and undergoes third-party audits to confirm security and compliance.

The in-scope system and supporting infrastructure is hosted by AWS. As such, AWS is responsible for the physical security controls for the in-scope system. Refer to the "Subservice Organizations" section below for controls managed by AWS.

<u>Logical Access</u>

SailPoint has documented and implemented policies and procedures for granting user access rights based on the minimum amount of access needed for their job classification.

SailPoint has procedures in place for user provisioning and maintenance for granting access to systems and services. User-access requests are managed through an automated system, including routing to the appropriate channels for provisioning and de-provisioning, to help ensure that specific elements of the onboarding and offboarding process are executed, including revoking system privileges. Access changes must be reviewed and approved by the appropriate owner.

SailPoint has established documented password standards that are posted within SailPoint's policy portal. SailPoint's password requirements include the following:

- Password changes at regular intervals
- Minimum characters
- Lockout after a number of invalid attempts
- Complexity requirements

The hosted solution provides options for integration with customers' existing authentication mechanisms using LDAP and SAML. An out of the box LDAP directory is included that is configured with password controls. SailPoint's customers are in full control of how they would like their access controls implemented.

Remote connections to production environments are through approved IPSEC VPN or TLS VPN.

SailPoint conducts quarterly access reviews to verify user access to systems and applications based on what is minimally necessary to support business activities.

Computer Operations - Backups

SailPoint maintains documented policies and procedures to guide personnel in backup and recovery activities and timeframes. SailPoint performs backups or has implemented failover technology of critical operational data and configurations within AWS. SailPoint leverages AWS automatic backups and schedules them to occur daily. Data backups are retained according to a pre-defined retention schedule.

Computer Operations - Availability

Documented policies and procedures are in place to guide employees in incident management activities to help ensure that systems are maintained and help ensure availability. Incidents are reported, recorded, managed, and appropriately communicated through a designed process. Security Administrators are responsible for ensuring the incident is recorded and tracked to resolution. Incidents are classified by priority and category by type or service (i.e., hardware application) and follow a formal escalation process.

SailPoint leverages cloud-based tools to monitor the capacity utilization of physical and computing metrics for customers to ensure that service delivery matches service level agreements. Capacity monitoring includes, but is not limited to, the following:

- Fargate Central Processing Unit (CPU) Utilization
- Fargate Memory Utilization
- Fargate Network TX
- Fargate Network RX
- RDS CPU Utilization
- RDS DB Connection Count
- RDS Storage Space
- RDS Freeable Memory
- RDS Write IOPS
- RDS Read IOPS
- Elasticache CPU Utilization
- Elasticache Database Memory Utilization
- Elasticache Cache Hit Rate
- Elasticache Memory Fragmentation Ratio
- Elasticache Network TX
- Elasticache Network RX
- Elasticache Freeable Memory
- Elasticache Evictions
- Elasticache Replication Lag

Change Control

Changes follow an established change management process. Changes are requested, documented, approved, and closed within SailPoint’s ticketing system. Production change requests are classified into priority categories. SailPoint has defined requirements for rollout procedures to implement approved changes into the production environment based on priority category. Change windows are pre-defined and communicated to customers in the event their service will be impacted. Changes are tested in an environment separate from production prior to implementation. Test environments mirror production as closely as possible to ensure change testing yields valid result.

The Application development team has an established process for branching source for new developments, testing, and code reviews. Code is developed on controlled company resources and stored in a private source control application. The source code repository maintains a history log of when code is committed, and the user associated with the activity. Changes to source code result in the creation of a new commit of application code, thus providing the capability of being rolled back to prior versions on an as needed basis. Developers do not have the access required to independently promote source code into the production environment.

Data Communications

SailPoint has integrated monitoring controls and tools into the daily function of SailPoint to provide continuous oversight into the security of SailPoint's products. The effectiveness of these controls is internally assessed through internal risk assessment activities.

SailPoint's production environment leverages AWS' security capabilities and services to increase privacy and control network access including but not limited to:

- Network firewalls
- Web application firewalls
- Image Scanning
- CloudWatch
- AWS Shield Protection
- Controlled access to SailPoint's instances and applications

SailPoint utilizes AWS available controls, configurations, and availability zones to build redundancy into the system infrastructure to help ensure there is no single point of failure.

Penetration tests against the production network, application and API are conducted on an annual basis by an external third-party in accordance with the vulnerability management policy. The purpose of this test is to ensure that systems are patched and properly and hardened against attacks from the internet. On a monthly basis, SailPoint performs application vulnerability scans. Vulnerability scanning is also performed through the SDLC and performed prior to the application moving to production. AWS Image scanning is enabled and set to scan on each push to ECR. Identified vulnerabilities are remediated according to SailPoint's vulnerability management policy.

The VPN system is configured to require users to connect via SSO using AD accounts. VPN access is restricted to authorized users only via AD groups and access is revoked as part of the termination process.

Boundaries of the System

The scope of this report includes the Non-Employee Risk Management Services provided at the remote facilities.

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Changes to the System in the Last 12 Months

On January 12, 2023, SailPoint acquired SecZetta, Inc. and its proprietary Third-Party Identity Risk Programs' Software-as-a-Service (SaaS) Service, which is now referred to as Non-Employee Risk Management. During the period, the predecessor organization's executive leadership team transitioned over from their previous roles into SailPoint Technologies, Inc.'s organizational structure, the overall responsibility for the System falls under SailPoint's Product Organization. There were no other changes likely to affect report users' understanding of how the Non-Employee Risk Management Services were used to provide the service during the review period to describe.

Incidents in the Last 12 Months

No significant incidents have occurred to the services provided to user entities in the 12 months preceding the end of the review period.

Criteria Not Applicable to the System

All Common/Security and Confidentiality criterion were applicable to the Non-Employee Risk Management Services.

Subservice Organizations

This report does not include the cloud hosting services provided by AWS at multiple facilities.

Subservice Description of Services

AWS provides cloud hosting services, which includes implementing infrastructure and physical security controls to protect the housed in-scope systems. AWS' Infrastructure security controls allows SailPoint to deploy and manage containers without the overhead of scaling, patching, securing, or managing servers. Physical controls include, but are not limited to, visitor sign-ins, required use of badges for authorized personnel, and monitoring and logging of physical access to the facilities.

Complementary Subservice Organization Controls

SailPoint's services are designed with the assumption that certain controls will be implemented by the subservice organization. Such controls are called complementary subservice organization controls. It is not feasible for all of the trust services criteria related to SailPoint's services to be solely achieved by SailPoint control procedures. Accordingly, the subservice organization, in conjunction with the services, should establish their own internal controls or procedures to complement those of SailPoint.

The following subservice organization controls should be implemented by AWS to provide additional assurance that the trust services criteria described within this report are met:

Subservice Organization - AWS		
Category	**Criteria**	**Control**
Common Criteria / Security	CC6.1	Password configuration settings are managed in compliance with Amazon.com's Password Policy.
		IT access above least privileged, including administrator accounts, is approved by appropriate personnel prior to access provisioning.

	CC6.1;
	CC6.6;
	CC6.7;
	CC7.1;
	CC7.2
		Virtual hosts are behind software firewalls which are configured to prevent Transmission Control Protocol (TCP) / Internet Protocol (IP) spoofing, packet sniffing, and restrict incoming connections to customer-specified ports.

	CC6.3	IT access privileges are reviewed on a periodic basis by appropriate personnel.
	CC6.4; CC7.2	Physical access to data centers is approved by an authorized individual.
		Physical access is revoked within 24 hours of the employee or vendor record being deactivated.

Subservice Organization - AWS		
Category	**Criteria**	**Control**
		Physical access to data centers is reviewed on a quarterly basis by appropriate personnel.
		Physical access points to server locations are recorded by closed circuit television camera (CCTV). Images are retained for 90 days, unless limited by legal or contractual obligations.
		Physical access points to server locations are managed by electronic access control devices.
		Electronic intrusion detection systems are installed within data server locations to monitor, detect, and automatically alert appropriate personnel of security incidents.

	CC6.8;
	CC7.1;
	CC7.2;
	CC8.1
		AWS performs deployment validations and change reviews to detect unauthorized changes to its environment and tracks identified issues to resolution.

To ensure AWS delivers on their service commitments, SailPoint carries out activities to monitor the subservice organization including but not limited to the following:

- SailPoint has access to several AWS dashboards which allow Security Administrators to centrally monitor availability and band-width trends
- AWS obtains a SOC 2 report that SailPoint reviews on an annual basis
- An annual risk assessment is completed to validate AWS continues to implement and maintain expected controls

COMPLEMENTARY USER ENTITY CONTROLS

SailPoint's services are designed with the assumption that certain controls will be implemented by user entities. Such controls are called complementary user entity controls. It is not feasible for all of the Trust Services Criteria related to SailPoint's services to be solely achieved by SailPoint control procedures. Accordingly, user entities, in conjunction with the services, should establish their own internal controls or procedures to complement those of SailPoint's.

The following complementary user entity controls should be implemented by user entities to provide additional assurance that the Trust Services Criteria described within this report are met. As these items represent only a part of the control considerations that might be pertinent at the user entities' locations, user entities' auditors should exercise judgment in selecting and reviewing these complementary user entity controls.

1. User entities are responsible for understanding and complying with their contractual obligation to SailPoint.
2. User entities are responsible for ensuring controls are in place that ensure the administration of the Non-Employee Risk Management Services for user entity personnel and authorized users is restricted based on job role and responsibility.
3. User entities are responsible for provisioning user access through appropriate security measures.
4. User entities are responsible for managing user accounts with access to in-scope applications, including those managed through their identity providers.
5. User entities are responsible for managing the roles and permissions that user accounts with access to the in-scope applications are provisioned, including those managed through their identity providers.

6. User entities are responsible for managing the passwords and authentication mechanisms that users with access to the in-scope applications utilize to gain access, include those managed through their identity providers.
7. User entities are responsible for ensuring controls are in place to manage the data entered into the system.
8. User entities are responsible for ensuring controls are in place that ensure that the customer has procedures in place for developing, maintaining, and testing their own business continuity plans.
9. User entities are responsible for ensuring controls are in place for protecting endpoints to thwart malicious software from entering the Non-Employee Risk Management Services cloud environment.
10. User entities are responsible for ensuring controls are in place for immediately notifying SailPoint of suspected or confirmed security breaches such as compromised accounts or passwords.