



Annette Lam  
Director, Compliance Program Management  
SailPoint Technologies Inc.  
11120 Four Points Drive,  
Suite 100, Austin, TX 78726 USA  
23 December 2024

Re: SailPoint IdentityNow Platform IRAP Assessment and Supplementary Assessment

Dear Ms Lam,

In October 2022, SailPoint Technologies Inc. engaged Anchoram Consulting to provide an Infosec Registered Assessors Program (IRAP) Assessment of perform an InfoSec Registered Assessors Program (IRAP) Assessment for the SailPoint Software as a Service (SaaS) and its supporting infrastructure against the PROTECTED information classification. The objective of this IRAP Assessment was to provide SailPoint and Australian Government cloud consumers an assessment of the effectiveness of the implementation of security controls necessary for authorising systems to hold and process Australian government information classified up to and including PROTECTED.

*Supplementary Assessment:*

In May 2024, SailPoint engaged Anchoram to undertake Supplementary assessment of SailPoint's Data Access Security (DAS) service which is a new cloud service addition to its 'Identity Security Cloud' Platform product. SailPoint DAS, as part of SailPoint Identity Security Cloud and Atlas SaaS Service, provides Data Access Governance solutions to clients in a variety of industries, including energy, financial services, healthcare, insurance, and the public sector. The supplementary assessment was also undertaken using the September 2022 ISM version.

We have completed the IRAP Assessment (the Assessment), in accordance with the Australian Signals Directorate's December 2020 IRAP Policy and Procedures and using the September 2022 version of the Australian Government Information Security Manual (ISM) for the controls recommended for PROTECTED security classification. The assessment, at a high level, entailed:

- Gaining an understanding of system architecture of the system being assessed
- Ensuring required physical security certifications have been attained
- Ensuring that appropriate security controls are selected, implemented and operating effectively
- Proposing mitigation strategies for any security controls that are not as effective as planned, and
- Enabling the reviewer of the report to make an informed risk-based decision about the system's suitability for their security needs and risk appetite.

Specifically, we undertook the following:

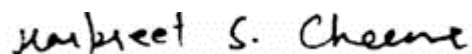
- Full system documentation review
- Interview(s) with key staff, including system owners, operations staff and stakeholders.
- Evidence gathering and verifying technical configurations to confirm effectiveness of security controls.

The assessment was undertaken by Harpreet (Harry) Cheema and Nathan Su, who are both listed on the Australian Cyber Security Centre's register of IRAP Assessors (<https://www.cyber.gov.au/resources-business-and-government/assessment-and-evaluation-programs/infosec-registered-assessors-program/irap-assessors> ). Supplementary assessment work was undertaken by Harry Cheema only.

The findings and recommendations including information about the alternate security controls can be found in the **SailPoint SaaS Service Cloud Security Assessment – Security Fundamentals and Cloud Services Assessment FINAL Report and Supplementary Assessment** Version 2.0 dated 23 December 2024 (SailPoint SaaS Service IRAP Report). SailPoint's cloud consumers should consider their own risk when using SailPoint's SaaS Service solution and understand their responsibilities under a 'Shared Responsibilities Model', also noted in the SailPoint SaaS Service IRAP Report. Anchoram Consulting's IRAP assessors assessed the implementation effectiveness of the security controls within the SailPoint SaaS Service and supporting infrastructure. Deviations from control guidelines have been identified, reviewed, and assessed. This assessment is designed to provide the relevant authorities, with sufficient information to consider the risks associated with enabling an Information Communication and Technology (ICT) solution. These associated risks should be considered as part of the assessment and Authority to Operate.

We thank SailPoint for the opportunity to work on this important initiative and recommend that SailPoint should review the assessment findings and address them with a clear Plan of Actions and Milestones. We also recommend that SailPoint should continue to keep itself up to date with the latest ISM guidelines and work with its consumers to ensure any material changes that may impact the security of SailPoint SaaS Service's security posture are considered, and adequate remediation measures are undertaken. As per our discussions with your team, SailPoint can maintain the validity and accuracy of the SailPoint SaaS Service IRAP Report through the addendums that can be added.

Best regards,

A handwritten signature in black ink that reads "Harpreet S. Cheema". The signature is written in a cursive, slightly slanted style.

Harpreet (Harry) Cheema, CISA, CISSP, IRAP Assessor  
Partner, Anchoram Consulting