+33 (0)1 48 10 09 46
formation@ambient-it.net
140 Avenue Jean Lolive 93500 Pantin - France

Updated on 03/19/2026

Sign up

SailPoint Identity Security Leader Certification Training

3 days (21 hours)

Overview

The SailPoint Identity Security Leader certification validates your ability to lead an Identity Security strategy and align risk, compliance, and operational efficiency. It is designed for contexts involving access governance, privilege reduction, and the standardization of identity processes.

This training provides structured preparation for the certification requirements: key IGA concepts, the responsibilities of an Identity Leader, and the relationship between policies, processes, and controls. The goal is to be able to explain, prioritize, and defend architecture and governance choices (joiner/mover/leaver, recertifications, SoD, RBAC/ABAC) to stakeholders.

The approach is resolutely practical: scoping workshops, case studies, guided demos, and exam-style quizzes. You'll leave with reusable deliverables: a roadmap template, risk/control matrix, RACI matrix, and assessment preparation checklist.

Like all our training courses, this one will introduce you to **the latest stable version** of the technology and its new features.

Objectives

- Explain the fundamentals of Identity Security and IGA.
- Map stakeholders, roles, and responsibilities (RACI).
- Define a governance strategy: JML, recertifications, SoD, roles.
- Prioritize a risk-oriented roadmap and metrics (KPIs/KRIs).
- Prepare for the assessment using sample questions and scenarios.

Target Audience

- IAM/IGA Managers
- CSOs, GRC, Risk Managers

Prerequisites

- Basic understanding of identity and access management (IAM/SSO/MFA)
- Understanding of compliance and audit requirements (e.g., ISO 27001, SOX, GDPR)
- Basic knowledge of authorization models (RBAC, privileges)
- Experience coordinating between IT, security, and business units

Technical requirements

- PC/Mac with at least 8 GB of RAM (16 GB recommended)
- Windows 10/11, macOS, or Linux, with a modern browser (Chrome/Edge/Firefox)
- Office suite for workshops (notes, tables, diagrams)
- Access to a functional video and audio conferencing tool if attending remotely

Our SailPoint Identity Security Leader Credential Certification Training Program

[Day 1 - Morning]

Fundamentals of Identity Security and SailPoint’s Positioning

- Clarifying IAM vs. IGA objectives: identity, access, governance, compliance
- Mapping risks: orphaned accounts, over-provisioning, excessive privileges, shadow IT
- Understanding key concepts: join/move/leave, roles, policies, attestations
- Identifying stakeholders: IT, security, HR, audit, business units, and responsibilities
- Hands-on workshop: Building a risk and stakeholder map for a typical IT system.

[Day 1 - Afternoon]

SailPoint architecture and governance capabilities

- Positioning the building blocks: identity sources, applications, connectors, workflows, governance
- Defining the identity model: attributes, correlation, data quality, and repositories
- Understanding provisioning vs. access requests vs. certification
- Introducing controls: SoD, access policies, exceptions, and compensations
- Hands-on workshop: Describing a target SailPoint architecture and its workflows

[Day 2 - Morning]

Access governance: roles, policies, and separation of duties

- Building a role model strategy: business roles, IT roles, entitlements
- Implementing policies: eligibility rules, safeguards, exceptions, and approvals
- Defining and implementing SoD: conflicts, rules, remediation, and traceability
- Measuring maturity: role coverage indicators, exception rates, access deviations
- Hands-on workshop: Design a mini-role model and a SoD rule for a business case.

[Day 2 - Afternoon]

Identity lifecycle and automation (JML)

- Define the Joiner/Mover/Leaver scenarios and their triggers (HR, ITSM, events)
- Define provisioning rules: default permissions, conditional permissions, revocation
- Manage technical and non-human accounts: ownership, rotation, controls
- Integrate processes: access requests, approvals, escalations, SLAs
- Hands-on workshop: Write a target JML workflow with steps, controls, and audit points.

[Day 3 - Morning]

Certifications, audits, and compliance reporting

- Structuring a certification campaign: scope, population, frequency, responsible parties
- Defining decisions and evidence: retain, revoke, delegate, comment, justify
- Optimizing efficiency: segmentation, risk-based prioritization, sampling, follow-ups
- Preparing for the audit: audit trails, logging, reports, and compensating controls
- Hands-on workshop: Designing a risk-based attestation campaign and its audit deliverables.

[Day 3 - Afternoon]

Leadership, deployment strategy, and preparation for certification

- Defining a roadmap: quick wins, batches, dependencies, success criteria
- Managing adoption: communication, training, RACI, product and run governance
- Establishing KPIs: reduction in over-provisioning, JML timelines, revocation rates, compliance
- Preparing for the exam: key topics, common pitfalls, answering techniques, and time management
- Hands-on workshop: Mock exam (scenario-based questions) and personalized revision plan.

Target Audience

This training is intended for both individuals and companies, large or small, wishing to train their teams in new advanced IT technologies or to acquire specific business knowledge or modern methods.

Assessment upon enrollment

The assessment conducted at the start of the training program complies with Qualiopi quality standards. Upon final registration, the learner receives a self-assessment questionnaire that allows us to evaluate their estimated proficiency with various types of technology, as well as their expectations and personal goals for the upcoming training, within the constraints of the selected format. This questionnaire also allows us to anticipate certain connection or internal security issues within the company (intra-company or virtual classroom) that could pose challenges for monitoring and ensuring the smooth running of the training session.

Teaching Methods

Practical Course: 60% Practical, 40% Theory. Training materials distributed in digital format to all participants.

Organization

The course alternates between theoretical input from the trainer, supported by examples and reflection sessions, and group work.

Assessment

At the end of the session, a multiple-choice questionnaire is used to verify that the skills have been properly acquired.

Certification

A certificate will be issued to each trainee who has completed the entire training program.