SAILPOINT IMPLEMENTATION CHECKLIST

For technical leaders evaluating or implementing SailPoint for the first time. 13 decision points that determine implementation success. These are the architecture, governance, and go-live choices GCA sees first-time teams get wrong. Each is a conversation worth having before you start building. Estimated timeline: 8-16 weeks for full SailPoint deployment.

SailPoint is the market leader in identity governance, but the platform is only as strong as the implementation behind it. A role model that is over-engineered collapses under its own weight. A certification campaign scoped too broadly produces rubber-stamp approvals. A connector strategy that skips standard connectors creates months of custom development. This checklist

covers the 13 decision points where GCA's SailPoint practice sees the most friction, the most rework, and the most avoidable risk.

These are not steps in a process. They are decisions that affect each other. A choice you make about role modeling will reshape your certification campaign design. Check off the items you have completed to track your progress. Expand each item for details and common mistakes.

01

These four decisions define the scope of your SailPoint deployment. Get the population count wrong and your licensing doubles mid-project. Miss an application and your connector timeline slips by months.

1

Identity Population Sizing

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Count every identity that SailPoint will govern: employees, contractors, service accounts, shared accounts, and non-employee populations. The number drives connector sizing, task scheduling, database capacity, and licensing.

> **Common mistake:** Counting only employees and discovering mid-project that contractor populations double the scope.

2

Application Inventory

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Governance*

Map every application that needs provisioning, deprovisioning, or access certification. Include the authoritative source (HR system, procurement), target systems (directories, SaaS, databases), and any applications with custom connectors.

> **Common mistake:** Starting with the "top 20" applications and discovering 80 more during

connector development.

3

Regulatory Scope

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Governance*

Identify which compliance frameworks apply to your identity program: SOX, HIPAA, PCI-DSS, NERC CIP, NIST 800-53. Each framework has specific requirements for access certification cadence, evidence retention, and segregation of duties.

Common mistake: Designing governance for "general best practice" and retrofitting regulatory alignment after go-live.

4

Platform Choice: IIQ vs ISC

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Decide whether SailPoint IdentityIQ (on-premises) or Identity Security Cloud (SaaS) is the right platform. The decision depends on data residency requirements, existing infrastructure, customization depth, and operational model. This is not a reversible choice mid-deployment.

Common mistake: Choosing ISC for cost reasons without evaluating the connector gaps for on-premises applications that require Virtual Appliances.

02

These five decisions shape how SailPoint operates at scale. An over-engineered role model becomes unmaintainable. An under-scoped connector strategy creates technical debt that compounds with every platform upgrade.

5

Connector Strategy

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Operations*

For each target application, decide: standard SailPoint connector, custom connector via SDK/ECMA, or file-based integration. Standard connectors are faster to deploy but may not support your application's specific attributes. Custom connectors give full control but add maintenance burden.

> **Common mistake:** Building custom connectors for applications where the standard connector covers 90% of the use case.

6

Role Model Design

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Decide how you will model access: business roles, application roles, permission roles, or a combination. The role model drives certification campaigns, SoD enforcement, and access request workflows. Over-engineered role models collapse under their own weight. Under-engineered ones produce certification fatigue.

> **Common mistake:** Building a role model that requires 400 roles for a 10,000-person organization. Start with 30-50 roles and expand based on certification feedback.

7

Certification Campaign Scope

STANDARD 2-4 HOURS (SINGLE WORKSHOP) *Governance*

Decide who reviews what, how often, and under what regulatory framework. Healthcare organizations scope certifications to PHI-handling applications. Financial services scopes to SOX-relevant systems. Not every application needs quarterly certification.

> **Common mistake:** Certifying every application on the same cadence, producing reviewer fatigue and rubber-stamp approvals.

8

Integration Mapping

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Map the integrations between SailPoint and adjacent platforms: PAM (CyberArk, BeyondTrust), federation (Ping, Okta, Entra), ITSM (ServiceNow), SIEM (Splunk, Sentinel), and HR systems. Each integration has authentication, data flow, and error handling requirements.

> **Common mistake:** Treating integrations as Phase 2 work and discovering at go-live that provisioning requires a PAM integration that was never scoped.

9

AI Governance Configuration

CRITICAL 1-2 WEEKS (DEPENDS ON SCOPE) *Security*

Decide whether to enable SailPoint's AI-powered governance features: access recommendations, anomaly detection, and policy suggestions. Configure recommendation thresholds, approval workflows, and exception handling. These features are available in Identity Security Cloud and can augment human governance decisions when tuned correctly. Note: AI governance features are not available in IdentityIQ. IIQ implementations rely on rule-based policies and manual certification workflows.

> **Common mistake:** Enabling AI features with default thresholds and overwhelming reviewers with low-confidence recommendations that erode trust in the system.

03

These four decisions determine whether your SailPoint deployment produces audit-ready governance or a platform nobody trusts. Connector failures that go undetected erode confidence. Certification deadlines that slip create compliance findings.

10

Test Evidence Packages

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Before go-live, produce test evidence that satisfies audit requirements: provisioning workflow results, certification behavior validation, SoD policy enforcement, and lifecycle event handling. This evidence must be available on day one of production, not built retroactively.

> **Common mistake:** Testing the happy path only and discovering failure modes (expired certificates, orphaned accounts, rejected provisioning) in production.

11

Parallel Run Plan

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Governance*

Run SailPoint alongside your existing access management process for a defined period before full cutover. The parallel run validates correlation, attribute authority, and provisioning accuracy against real production patterns.

> **Common mistake:** Skipping the parallel run to hit a go-live date, then spending months reconciling discrepancies between SailPoint and the legacy process.

12

Audit Continuity

CRITICAL 2-4 HOURS (SINGLE WORKSHOP) *Operations*

If your organization is under regulatory audit, plan how the certification cadence, SoD enforcement, and evidence stream transition from the legacy process to SailPoint. Regulated organizations cannot pause their compliance program for a platform change.

> **Common mistake:** Migrating mid-certification-cycle and producing evidence gaps that auditors flag as findings.

13

Managed Operations Handoff

STANDARD 1-2 WEEKS (DEPENDS ON SCOPE) *Operations*

Decide who operates SailPoint after go-live: internal team, GCA managed services, or hybrid. Define SLAs for connector health monitoring, certification campaign execution, access request queue management, and platform upgrades.

> **Common mistake:** Treating go-live as the finish line and discovering three months later that no one owns connector failures or certification deadlines.

These 13 decisions are SailPoint-specific in execution. When GCA is involved, here is how we approach them differently.

We scope the architecture against your identity population, application landscape, and regulatory requirements before any configuration begins. GCA holds SailPoint's Delivery Admiral competency and is rated 4.8 / 5.0 on Gartner Peer Insights based on 32 verified reviews. Our SailPoint practice covers IdentityIQ, Identity Security Cloud, NERM, and the full IIQ-to-ISC migration path. See our full identity governance practice for the broader IGA landscape beyond SailPoint.

DOWNLOAD SAILPOINT CHECKLIST (PDF)

SAILPOINT PARTNER PAGE

BOOK A CONSULTATION

Need help with your SailPoint Implementation Checklist?

GCA Technology Services — gca.net — Book a consultation: gca.net/book-a-consultation

MANAGING YOUR DIGITAL IDENTITIES

SERVICES

Managed IAM

Implementation

Assessment & Strategy

General IAM

SOLUTIONS

Identity Management

Web Access Management

Identity Governance

Privileged Access

PARTNERS

SailPoint

Microsoft Entra

Okta

OpenText

Netwrix

Ping Identity

COMPANY

About GCA

Careers

Contact Us

Privacy Policy

expressed or implied, with respect to this content, about its accuracy or completeness, including any warranties of merchantability or fitness for a particular purpose.