SailPoint Governance & Compliance Coverage Scorecard

How much of your governance model is actually centralized through SailPoint?

Many organizations assume SailPoint is their system of record for access governance because certifications run and key connectors are live. But critical business applications, administrative channels, lifecycle processes, and audit evidence often remain outside governed scope. Teams are left relying on spreadsheets, email approvals, screenshots, local workarounds, and disconnected evidence to satisfy audit, SOX, and regulatory requirements.

This scorecard helps you quantify that gap across the five areas that matter most for audit, regulatory compliance, and access risk: **application coverage, access certification quality, audit evidence strength, process integrity, and business adoption.**

HOW TO USE THIS SCORECARD

For each statement, mark the score that best reflects your current environment.

0	Not true	1	Mostly not true	2	Partly true
3	Mostly true	4	Fully true	N/A	Genuinely doesn't apply

Add the subtotals for each section, then calculate your total out of 100. If you use N/A, normalize:

Normalized score = (points earned ÷ maximum available points for applicable statements) × 100

01 Application coverage — 20 POINTS

If SailPoint governs only a narrow portion of high-risk systems, centralized governance is incomplete.

1	SailPoint-centered governance extends to most high-risk and high-audit-impact applications, not just the directory and a few core systems.	0	1	2	3	4	N/A

2	Finance, HR, operational, clinical, regional, legacy, acquired, industry-specific, custom, and business-owned applications are included in the governance model, even if they aren't all provisioned directly through SailPoint.	0	1	2	3	4	N/A
3	Access granted through administrative channels, service desks, other provisioning tools, and direct application changes is visible within the broader governance model.	0	1	2	3	4	N/A
4	The organization can clearly identify which critical systems are inside governed scope and which are still managed through local processes.	0	1	2	3	4	N/A
5	High-risk systems outside SailPoint are tracked as named governance gaps with clear ownership, risk classification, and remediation plans.	0	1	2	3	4	N/A

APPLICATION COVERAGE SUBTOTAL _____ / 20

02 Access certification quality

20 POINTS

Access certifications reduce risk only when reviewers can see meaningful entitlements, understand the business context, and make decisions within a governed workflow.

1	Managers reviewing access can see the underlying entitlements and privileges that create business or financial risk, not just high-level role names.	0	1	2	3	4	N/A
2	Access certifications cover the entitlements and privileges that matter for audit, regulatory compliance, and security decisions.	0	1	2	3	4	N/A
3	Certification decisions are made in SailPoint or connected governed workflows rather than through spreadsheets, email threads, or offline files.	0	1	2	3	4	N/A
4	Reviewers have enough business context — entity, business unit, location, function, legal structure, or data access — to make informed approval decisions.	0	1	2	3	4	N/A

5	The organization could provide current certification evidence to auditors without extensive manual explanation, reconciliation, or offline support.	0	1	2	3	4	N/A
6	Reviewers can distinguish genuine high-risk access from technical conflicts or false positives.	0	1	2	3	4	N/A

ACCESS CERTIFICATION SUBTOTAL _____ / 20

03 Audit evidence strength

20 POINTS

If auditors still need screenshots, local extracts, and manual reconciliations, SailPoint isn't yet supporting a complete and reliable evidence model.

1	Evidence for access, approvals, certifications, SoD, lifecycle events, exceptions, and remediation can be traced across governed systems without relying heavily on screenshots or ad hoc extracts.	0	1	2	3	4	N/A
2	Auditors can see who approved access, what policies and SoD checks were applied, and how exceptions or remediation were handled.	0	1	2	3	4	N/A
3	Evidence is consistent across SailPoint, ticketing systems, provisioning tools, and application-level records.	0	1	2	3	4	N/A
4	Audit and compliance teams can rely on governance data as a primary evidence source rather than treating it as one incomplete input among many.	0	1	2	3	4	N/A
5	SOX, regulatory, and internal audit testing no longer depend on repeated spreadsheet reconciliations and local data pulls for critical applications.	0	1	2	3	4	N/A

6	Evidence connects the access request, approval, SoD evaluation, remediation, provisioning outcome, and final sign-off into one complete audit trail.	0	1	2	3	4	N/A

AUDIT EVIDENCE SUBTOTAL _____ / 20

04 Process integrity

20 POINTS

Parallel approvals, side workflows, and local exceptions weaken control consistency even when SailPoint is technically in place.

1	Access approvals follow defined workflows instead of parallel email chains, shared files, or local approval practices.	0	1	2	3	4	N/A
2	Joiner, mover, and leaver processes are governed consistently across critical systems, including systems outside direct SailPoint provisioning paths.	0	1	2	3	4	N/A
3	The organization can verify that access is updated or removed promptly after transfers, role changes, and terminations across both SailPoint and non-SailPoint applications.	0	1	2	3	4	N/A
4	SoD checks identify meaningful conflicts, filter false positives, and evaluate risk across critical applications without relying on separate spreadsheets or local workarounds.	0	1	2	3	4	N/A
5	Elevated and privileged access is visible, reviewed, and monitored through a defined governance process, and teams can identify where manual processes still bypass it.	0	1	2	3	4	N/A
6	Preventive controls evaluate access before it is granted rather than relying only on periodic certification.	0	1	2	3	4	N/A

PROCESS INTEGRITY SUBTOTAL _____ / 20

05 Business adoption

20 POINTS

A governance model is only as strong as the business trust and participation behind it.

1	Business managers see SailPoint-based reviews as meaningful governance decisions, not just IT workflow tasks.	0	1	2	3	4	N/A
2	Reviewers trust the access data, entitlement detail, and business context presented during certification decisions.	0	1	2	3	4	N/A
3	Business teams don't maintain parallel approval logs, side spreadsheets, or separate review processes for critical applications.	0	1	2	3	4	N/A
4	IAM, audit, compliance, security, application owners, and business stakeholders share a common understanding of what is in scope and what evidence should exist.	0	1	2	3	4	N/A
5	Leadership can explain how SailPoint has improved governance outcomes in terms of risk, regulatory compliance, audit readiness, lifecycle control, and operational efficiency.	0	1	2	3	4	N/A
6	Business leaders can explain governance outcomes in terms of reduced audit effort, stronger compliance, lower risk, and faster access decisions rather than implementation metrics.	0	1	2	3	4	N/A

BUSINESS ADOPTION SUBTOTAL _____ / 20

Your total score

Application coverage	_____	Process integrity	_____
Access certification quality	_____	Business adoption	_____
Audit evidence strength	_____		

TOTAL SCORE _____ / 100

If you marked any statements N/A, use the normalized score formula on the first page.

Score interpretation

80–100

Strong governance and compliance foundation

SailPoint appears to support the center of a broader governance model, with solid coverage, stronger evidence, and good business participation. Gaps may still exist, but they're less likely to drive widespread manual reviews or undermine audit reliance.

60–79

Partial governance with a visible value gap

SailPoint is delivering value, but important gaps remain in application coverage, evidence quality, process consistency, or adoption. This is the range where teams often say, "We have SailPoint, but audit preparation and access certifications still feel manual."

40–59

Fragmented governance with limited compliance confidence

Your environment likely operates with a split model. SailPoint governs some access, while critical decisions and evidence still live in spreadsheets, email workflows, tickets, and local application processes. Audit reliance is limited, review quality is uneven, and the gap is visible to auditors and leadership.

Below 40

High audit exposure and low governance confidence

Your program likely has significant coverage blind spots, incomplete evidence chains, and heavy dependence on local processes. SailPoint may be deployed, but it isn't yet supporting consistent governance across audit, regulatory compliance, security, and the business.

What your score is telling you

A low score doesn't mean SailPoint was the wrong investment. It usually means the governance model around SailPoint never expanded to cover all the applications, access paths, lifecycle processes, evidence, and business decisions that matter for SOX, regulatory compliance, internal audit, and security.

The critical question isn't whether SailPoint is deployed. It's whether governance reaches the places where audit pressure, access risk, and manual effort still exist.

NEXT STEP

Request a SailPoint Governance Coverage Assessment

Use your scorecard results as the starting point for a structured review of:

- Which high-risk and high-audit-impact applications, provisioning paths, and administrative channels sit outside SailPoint-centered governance.
- Which manual workflows and parallel processes are creating inconsistent governance across the organization.
- Where your access, certification, SoD, lifecycle, and change evidence breaks and forces auditors back to spreadsheets, screenshots, and local data pulls.
- Which gaps create the greatest SOX, regulatory, audit, or access risk and should be addressed first.

The assessment turns your score into a practical roadmap for extending governance coverage, strengthening audit-ready evidence, and reducing manual work around your existing SailPoint deployment — without starting over with a new IGA program.

