



e-ISSN: 2319-8753 | p-ISSN: 2347-6710

IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 13, Issue 3, March 2024

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.423



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

SailPoint and ForgeRock Identity Governance Implementation Patterns for Multi-Agency Public Sector Access Management

Senthil Babu Malli Jayaraj

IT Project Manager, USA

ABSTRACT: Multi-agency public sector environments, in which a shared services organization, a state technology agency, or a consolidated identity platform serves dozens of individual agencies with distinct business processes and compliance obligations, present identity governance challenges that single agency implementations do not fully anticipate. SailPoint and ForgeRock, two of the identity governance and access management platforms most frequently deployed in public sector environments as of early 2024, offer materially different architectural approaches: SailPoint's IdentityIQ and IdentityNow products emphasize governance-first capabilities including access certification and role modeling, while ForgeRock's Identity Platform emphasizes API-driven orchestration and federation across a broader range of identity types, including citizen-facing identities. This research article compares SailPoint and ForgeRock implementation patterns for multi-agency public sector access management, examining capability tradeoffs across six governance dimensions, access certification design, role modeling approaches, and a five stage identity governance maturity model. Findings are illustrated with a distinct set of two-dimensional charts, including a lollipop comparison chart, a donut chart of certification outcomes, a step chart of provisioning time by maturity stage, and a diverging bar chart of risk reduction by control area, alongside extensive grid style and vendor-comparison data tables. Drawing on vendor technical documentation, public sector identity governance research, and access management standards literature published through February 2024, this article finds that agencies combining SailPoint's certification and role governance strengths with ForgeRock's federation and orchestration strengths, whether through a dual-platform architecture or a single platform supplemented by targeted integration, report more complete governance coverage than agencies relying on either platform's default capability set alone.

◇ VENDOR CONTEXT

This article compares SailPoint and ForgeRock at the level of documented product capability and common public sector implementation pattern. Specific version capabilities evolve over time, and agencies should confirm current capability against vendor documentation at the time of implementation planning.

KEYWORDS: SailPoint, ForgeRock, identity governance, access management, multi-agency, access certification, role modeling, segregation of duties, public sector IAM.

I. INTRODUCTION AND RESEARCH CONTEXT

State and federal technology agencies increasingly consolidate identity governance and access management functions to serve multiple client agencies from a shared platform, driven by both cost efficiency goals and the security benefits of centralized identity governance. This consolidation introduces requirements distinct from single agency identity management, including support for heterogeneous agency-specific role structures, varying compliance obligations, and, in many cases, both workforce and citizen-facing identity populations on the same platform.

◆ 1.1 Research Objectives

- **Objective 1:** Compare SailPoint and ForgeRock capability profiles across governance dimensions most relevant to multi-agency public sector deployment.
- **Objective 2:** Present access certification, role modeling, and federation design patterns suited to cross-agency identity ecosystems.
- **Objective 3:** Quantify illustrative risk reduction and provisioning efficiency outcomes associated with mature identity governance implementation.
- **Objective 4:** Provide a maturity model, governance structure, and implementation roadmap for multi-agency identity governance programs.

◆ 1.2 Scope and Methodology

This research draws on the following source categories, all published prior to March 2024:

- SailPoint and ForgeRock vendor technical documentation and published architectural guidance.
- Public sector identity governance research, including state and federal shared services identity platform case material.
- Access management and identity governance standards literature, including NIST digital identity guidelines.
- Academic and practitioner literature addressing role-based access control and segregation of duties design.

Multi-Agency Identity Requirement	Description	Single-Agency Contrast
Heterogeneous role structures	Each client agency may define roles and entitlements differently even for functionally similar positions.	A single agency typically maintains one consistent role taxonomy.
Varying compliance obligations	Different agencies may be subject to different federal program-specific or state statutory compliance requirements.	A single agency generally operates under one consistent compliance regime.
Mixed identity populations	The platform may serve workforce identities for multiple agencies alongside citizen-facing identities for public-facing services.	A single agency's identity population is typically more homogeneous.
Shared governance accountability	Governance decisions affecting the shared platform require coordination across multiple agency stakeholders.	A single agency's governance decisions rest with one accountable body.

◆ 1.3 Market Context for the Platform Comparison

SailPoint and ForgeRock were selected for comparison in this article because, as of the period leading into 2024, both were frequently referenced in public sector identity governance and access management procurement activity, though for partly different reasons reflecting the platform distinction described in Section 3.

Factor	Relevance to Public Sector Selection
FedRAMP and state authorization availability	Both platforms have pursued relevant public sector authorization pathways, a common procurement gating factor for state and federal agencies.
Existing agency footprint	Agencies already using one platform for a related function, such as workforce identity governance or citizen-facing authentication, often extend that existing footprint rather than introducing a net-new platform.
Analyst and peer reference availability	Both platforms appear regularly in analyst evaluations and public sector peer reference material, supporting procurement due diligence.
Systems integrator familiarity	Public sector systems integrators commonly supporting state technology modernization frequently maintain implementation practice around one or both platforms.

This article does not evaluate other identity governance and access management platforms present in the public sector market; the comparison is deliberately scoped to SailPoint and ForgeRock given their prevalence in the multi-agency deployment pattern this article examines.

II. THE MULTI-AGENCY IDENTITY GOVERNANCE PROBLEM

Before comparing specific platform capabilities, it is useful to characterize precisely what makes multi-agency identity governance structurally different from, and more difficult than, single agency identity governance.

◆ 2.1 Structural Challenges

- **Challenge 1: Role model heterogeneity.** A shared identity platform must accommodate each agency's distinct role and entitlement model without forcing artificial standardization that would misrepresent actual agency business processes.
- **Challenge 2: Certification configurability.** Access certification campaigns, examined further in Section 5, must be configurable per agency, since certification frequency and reviewer assignment logic reasonably differ by agency risk tolerance and staffing.
- **Challenge 3: Segregation of duties scoping.** Segregation of duties rules, examined in Section 6, are often agency-specific, yet the platform must enforce them consistently within each agency's context without cross-agency rule bleed.
- **Challenge 4: Cross-agency governance coordination.** Governance decisions affecting shared platform configuration require a cross-agency governance body, echoing coordination patterns seen in other multi-system public sector technology governance contexts.

◆ 2.2 Why Platform Choice Matters More at Multi-Agency Scale

In a single agency deployment, gaps in a given platform's capability can often be addressed through custom configuration or a small number of manual compensating processes. At multi-agency scale, the same capability gap multiplies across every client agency, making the underlying platform's native capability profile, examined in Sections 3 and 4, a significantly more consequential decision.

III. PLATFORM OVERVIEW: SAILPOINT AND FORGEROCK

SailPoint and ForgeRock originate from different points in the identity management market and reflect that origin in their respective architectural emphasis.

◆ 3.1 SailPoint Overview

Attribute	Description
Primary product lines	IdentityIQ (on-premises or hybrid deployment) and IdentityNow (cloud-native SaaS deployment).
Architectural emphasis	Governance-first design, with access certification, role modeling, and policy enforcement as core, mature capabilities.
Typical primary use case	Workforce identity governance, access certification campaigns, and audit-ready compliance reporting.
Typical integration approach	Connector-based integration with target systems, with a large library of pre-built connectors for common enterprise applications.

◆ 3.2 ForgeRock Overview

Attribute	Description
Primary product lines	ForgeRock Identity Platform, encompassing Access Management, Identity Management, Directory Services, and Identity Gateway components.
Architectural emphasis	API-driven orchestration, federation, and support for a broad range of identity types, including consumer and citizen-facing identities.
Typical primary use case	Federated single sign-on, citizen-facing digital service authentication, and API security across a heterogeneous application ecosystem.
Typical integration approach	Standards-based integration (SAML, OAuth 2.0, OpenID Connect) with orchestration trees enabling flexible authentication flow customization.

◇ VENDOR CONTEXT

Both platforms have expanded beyond their original emphasis over time; SailPoint has extended into cloud-native access management capability, and ForgeRock has extended governance capability. The comparison in Section 4 reflects each platform's traditionally stronger area as commonly deployed in public sector environments through early 2024, not an exhaustive feature-by-feature audit.

IV. CAPABILITY COMPARISON ACROSS SIX GOVERNANCE DIMENSIONS

A structured, dimension-by-dimension comparison clarifies where each platform's native strengths lie, informing the deployment architecture decisions examined in Section 9.

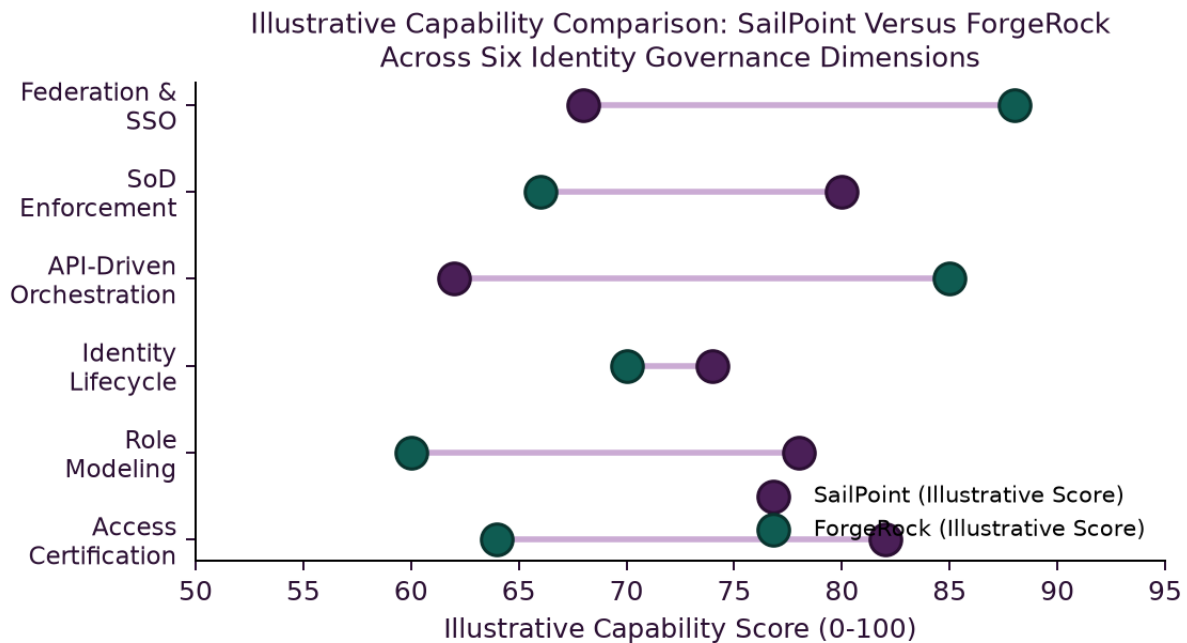


Figure 1. Illustrative capability comparison between SailPoint and ForgeRock across six identity governance dimensions.

◆ 4.1 Dimension-by-Dimension Comparison

Capability	SailPoint	ForgeRock
Access certification	Mature, purpose-built certification campaign management with configurable review workflows.	Present, with governance capability expanded in recent platform versions, though historically less mature than SailPoint's purpose-built certification tooling.
Role modeling	Mature role mining and modeling tooling supporting complex, multi-agency role taxonomies.	Present but historically less emphasized than SailPoint's role mining capability.
Identity lifecycle management	Strong joiner-mover-leaver workflow automation, particularly for workforce identities.	Strong for both workforce and citizen-facing identity types, reflecting the platform's broader identity type support.
API-driven orchestration	Present but less flexible than ForgeRock's orchestration tree model.	Highly mature, with a flexible orchestration tree model supporting complex, customizable authentication flows.
Segregation of duties enforcement	Mature, purpose-built segregation of duties rule engine with cross-application visibility.	Present, though historically less purpose-built for segregation of duties specifically compared to general access policy enforcement.
Federation and single sign-on	Present and functional, though federation is not the platform's primary architectural emphasis.	Highly mature, with deep standards-based federation support and strength in citizen-facing single sign-on scenarios.

◆ 4.2 Interpreting the Comparison

- **Pattern observed:** The dimension-by-dimension pattern in Figure 1 and Table 5 suggests a natural division of primary strength: SailPoint for governance-intensive functions (certification, role modeling, segregation of duties) and ForgeRock for orchestration-intensive functions (API-driven flows, federation).
- **Important qualification:** Neither platform's comparative weakness in Figure 1 should be read as an absence of the capability entirely; both platforms continue to invest in capability areas outside their traditional strength, per the vendor context note in Section 3.2.

V. ACCESS CERTIFICATION DESIGN PATTERNS

Access certification, the recurring process of reviewing and confirming that existing access remains appropriate, is a central governance function in multi-agency identity platforms and one of SailPoint's traditionally strongest capability areas per Section 4.1.

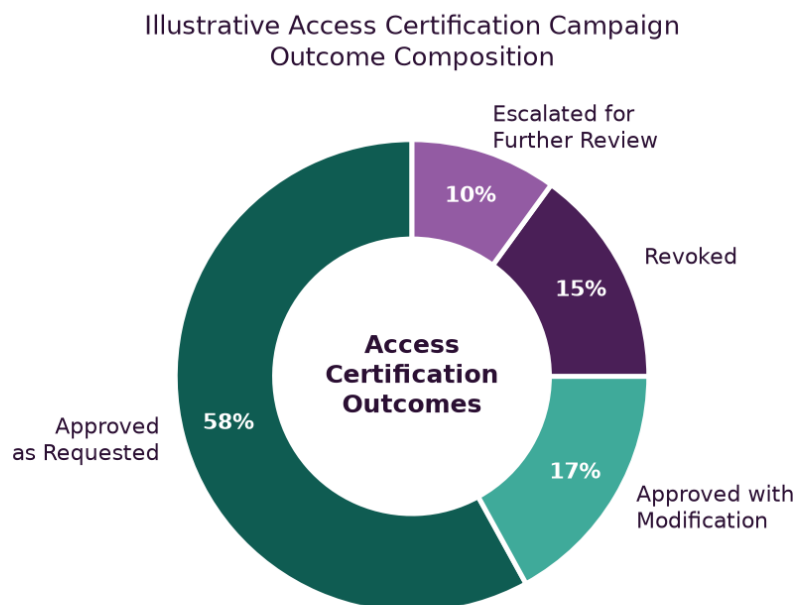


Figure 2. Illustrative access certification campaign outcome composition.

◆ 5.1 Certification Campaign Design Elements

Design Element	Description	Multi-Agency Consideration
Campaign scope	Defines which users, applications, or entitlements are included in a given certification campaign.	Should typically be scoped per agency to respect agency-specific risk tolerance and staffing capacity.
Reviewer assignment	Determines who reviews and approves or revokes each certification item, typically a manager or resource owner.	Reviewer hierarchy must respect agency-specific organizational structure, not a single shared hierarchy.
Certification frequency	Defines how often a given certification campaign recurs.	May reasonably vary by agency based on the sensitivity of that agency's data and applications.
Escalation and remediation workflow	Defines what happens when a reviewer flags an item or when a campaign deadline passes without action.	Escalation paths must route to the correct agency-specific accountable party.

◆ 5.2 Interpreting Certification Outcomes

As illustrated in Figure 2, a well-functioning certification campaign typically approves the majority of access as requested, consistent with the expectation that most existing access remains appropriate. The escalated for further review share, illustrated at 10 percent, and the revoked share, illustrated at 15 percent, together represent the portion of the campaign delivering the most direct governance value, surfacing access that would otherwise have persisted unexamined.

- **Governance signal:** A certification campaign with an unusually low revocation rate across multiple consecutive cycles may indicate reviewer fatigue or rubber-stamping rather than genuinely low-risk access, a pattern warranting closer governance attention rather than assumption of program success.

VI. ROLE MODELING AND SEGREGATION OF DUTIES

Role modeling and segregation of duties (SoD) enforcement work together to prevent both excessive individual privilege and toxic combinations of privilege across roles.

◆ 6.1 Role Modeling Approaches

Approach	Description	Best Suited Context
Top-down role design	Roles are defined based on documented job functions and business process analysis before implementation.	New agency onboarding where job functions are well documented in advance.
Bottom-up role mining	Roles are derived from analysis of actual, existing access patterns across the current user population.	Migrating an existing agency's access model into the shared platform without disrupting current operations.
Hybrid role modeling	Bottom-up mining establishes an initial baseline, refined through top-down business process validation.	Most multi-agency scenarios, balancing implementation speed against role accuracy.

◆ 6.2 Segregation of Duties Rule Scoping in Multi-Agency Environments

- **Scoping principle 1:** SoD rules should generally be scoped to a single agency's application and role context, since a toxic combination in one agency's context may not apply to another agency's distinct business processes.
- **Scoping principle 2:** Where agencies share a common application, such as a shared financial system, SoD rules governing that shared application should be defined once, centrally, rather than duplicated inconsistently by each agency.
- **Scoping principle 3:** SoD rule ownership should be assigned explicitly, distinguishing rules owned by the shared platform governance function from rules owned by individual agency business process owners.

VII. IDENTITY LIFECYCLE MANAGEMENT ACROSS AGENCY BOUNDARIES

Joiner-mover-leaver lifecycle management, the automated provisioning, modification, and de-provisioning of access as an individual's employment or role status changes, requires particular care at multi-agency scale given the possibility of an individual moving between agencies rather than simply joining or leaving employment altogether.

◆ 7.1 Lifecycle Event Types and Multi-Agency Handling

Lifecycle Event	Standard Handling	Multi-Agency Specific Consideration
Joiner	New identity created and initial access provisioned based on role.	Must correctly associate the identity with the specific hiring agency's role context.
Mover (within agency)	Access adjusted to reflect the new role within the same agency.	Generally handled identically to single-agency lifecycle management.
Mover (across agencies)	Access from the prior agency should generally be revoked while new agency access is provisioned.	Requires explicit cross-agency handoff logic; a common source of orphaned access if not deliberately designed.
Leaver	All access is de-provisioned upon confirmed departure.	Must confirm departure from all agencies where the individual held access, not just the agency initiating the leaver event.

◆ 7.2 The Cross-Agency Mover Risk

The cross-agency mover scenario in Table 8 deserves particular attention because it is the lifecycle event type most likely to be mishandled by identity platforms configured primarily around single agency assumptions. Absent explicit cross-agency handoff logic, an individual moving from one agency to another may retain their prior agency's access indefinitely, representing exactly the kind of orphaned access finding examined in the risk reduction data in Section 11.

VIII. FEDERATION AND SINGLE SIGN-ON ARCHITECTURE

Federation and single sign-on architecture determine how identities authenticate across the range of applications and services within a multi-agency ecosystem, an area of traditional strength for ForgeRock per Section 4.1.

◆ 8.1 Federation Pattern Comparison

Federation Pattern	Description	Best Suited Multi-Agency Scenario
Centralized identity provider	A single, shared identity provider authenticates users across all participating agencies.	Agencies willing to fully adopt a shared authentication standard and user experience.
Federated identity provider mesh	Each agency maintains its own identity provider, federated together through standards-based trust relationships.	Agencies with existing, mature identity infrastructure that should be preserved rather than replaced.
Hybrid broker model	A central identity broker mediates between agency-specific identity providers and consuming applications.	Environments with a mix of agencies at different modernization maturity levels.

◆ 8.2 Standards Underlying Federation

- **SAML:** Security Assertion Markup Language, a widely adopted federation standard particularly common in longer-established public sector identity federations.
- **OAuth 2.0:** An authorization framework enabling delegated access, commonly used to secure API access in modern, API-driven architectures.
- **OpenID Connect:** An authentication layer built on OAuth 2.0, providing standardized identity assertions commonly used in modern single sign-on implementations.

IX. DEPLOYMENT ARCHITECTURE PATTERNS

Given the complementary strength pattern identified in Section 4.2, several deployment architecture patterns have emerged for combining or selecting between SailPoint and ForgeRock capability in multi-agency environments.

◆ 9.1 Architecture Pattern Comparison

Pattern	Description	Primary Tradeoff
Single-platform, SailPoint-primary	SailPoint serves as the primary governance and access management platform; federation needs are addressed through SailPoint's native or supplementary capability.	Strong governance and certification capability; federation flexibility more limited than a dedicated federation-first platform.
Single-platform, ForgeRock-primary	ForgeRock serves as the primary platform; governance needs are addressed through ForgeRock's native governance capability.	Strong federation and orchestration flexibility; certification and role modeling capability historically less mature.
Dual-platform, integrated	Both platforms operate together, with ForgeRock handling authentication and federation while SailPoint handles governance and certification, integrated through standards-based interfaces.	Captures both platforms' primary strengths; introduces integration complexity and dual-platform operational overhead.

◆ 9.2 Selecting an Architecture Pattern

- **Consideration 1:** Agencies with a strong existing compliance and audit obligation, where certification quality is paramount, may find the governance capability gap in a ForgeRock-primary pattern more consequential than the integration overhead of a dual-platform pattern.
- **Consideration 2:** Agencies with a significant citizen-facing identity population, where federation flexibility and authentication user experience are paramount, may find the federation capability gap in a SailPoint-primary pattern more consequential.
- **Consideration 3:** The dual-platform pattern's integration complexity should not be underestimated; agencies pursuing this pattern should budget dedicated integration engineering effort, not treat integration as a minor implementation detail.

X. THE FIVE STAGE IDENTITY GOVERNANCE MATURITY MODEL

Multi-agency identity platforms can be classified into one of five maturity stages describing overall identity governance readiness, independent of the specific platform or architecture pattern chosen.

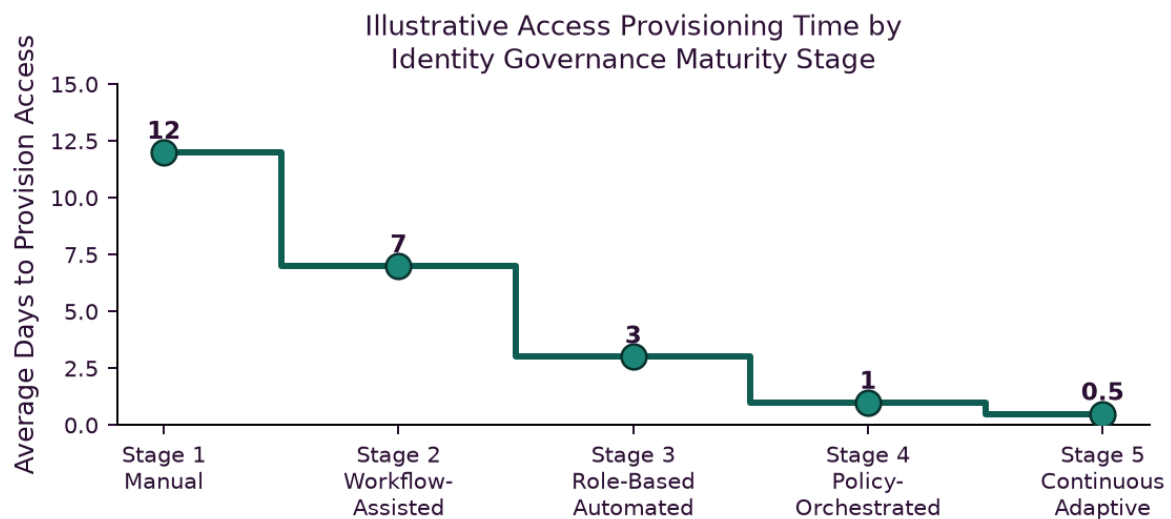


Figure 3. Illustrative access provisioning time by identity governance maturity stage.

Stage	Name	Description
1	Manual	Access requests and approvals are handled through manual, largely undocumented processes.
2	Workflow-Assisted	Basic workflow automation exists for access requests, but role modeling and certification remain manual.
3	Role-Based Automated	Role-based provisioning and basic certification campaigns operate, per Sections 5 and 6, across most agencies.
4	Policy-Orchestrated	Segregation of duties enforcement and federation architecture, per Sections 6 and 8, operate consistently across the full multi-agency ecosystem.
5	Continuous Adaptive	Access decisions incorporate continuous risk signals, with near-instantaneous provisioning and adaptive certification prioritization.

As illustrated in Figure 3, provisioning time declines sharply across successive maturity stages, from an average of 12 days at the Manual stage to under a day at the Continuous Adaptive stage, reflecting the cumulative effect of role-based automation, policy orchestration, and continuous risk-based decisioning.

XI. RISK REDUCTION OUTCOMES

Mature identity governance implementation is associated with measurable reduction in several recurring access-related risk finding categories.

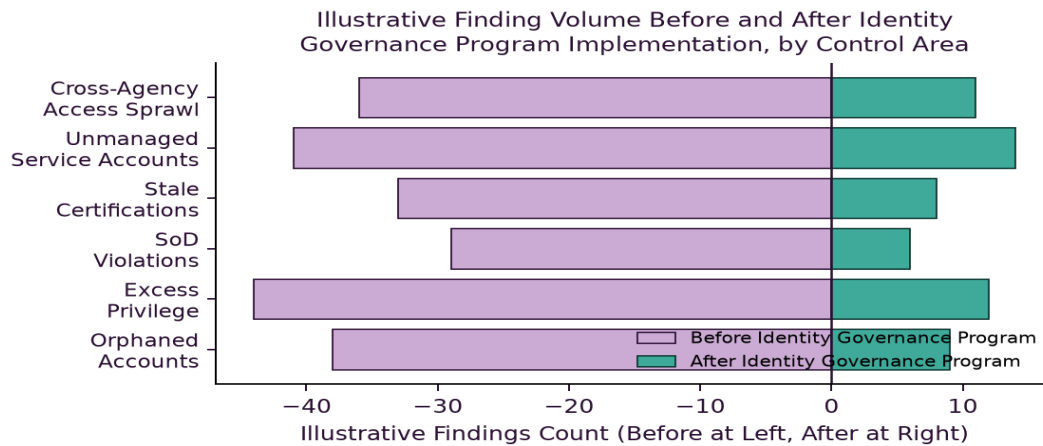


Figure 4. Illustrative finding volume before and after identity governance program implementation, by control area.

◆ 11.1 Risk Reduction Observations

Control Area	Illustrative Before Count	Illustrative After Count	Approximate Reduction
Orphaned accounts	38	9	Approximately 76 percent
Excess privilege	44	12	Approximately 73 percent
Segregation of duties violations	29	6	Approximately 79 percent
Stale certifications	33	8	Approximately 76 percent
Unmanaged service accounts	41	14	Approximately 66 percent
Cross-agency access sprawl	36	11	Approximately 69 percent

◆ 11.2 Interpreting the Pattern

- **Largest reduction:** Segregation of duties violations showed the largest illustrative proportional reduction, consistent with the purpose-built SoD rule engines examined in Section 6.2 directly targeting this specific finding category.
- **Smallest reduction:** Unmanaged service accounts showed the smallest illustrative proportional reduction, consistent with service accounts often falling outside standard joiner-mover-leaver lifecycle processes examined in Section 7, requiring deliberate, separate governance attention.
- **Persistent risk:** Cross-agency access sprawl's meaningful but comparatively moderate reduction is consistent with the cross-agency mover risk described in Section 7.2 remaining a persistent, harder-to-fully-eliminate risk category even in mature implementations.

XII. GOVERNANCE AND OPERATIONAL OWNERSHIP

Sustained identity governance effectiveness requires governance structures spanning both the shared platform operator and individual client agencies.

◆ 12.1 Governance Roles

Role	Primary Responsibility	Typical Organizational Home
Shared platform governance lead	Owns platform-wide configuration standards, shared connector management, and cross-agency SoD rule governance.	State technology agency or shared services organization.
Agency identity governance liaison	Owns agency-specific role definitions, certification campaign configuration, and agency-specific SoD rules.	Individual client agency, typically within IT or security.

Certification campaign owner	Schedules and monitors certification campaign completion per Section 5.	Either the shared platform or individual agency, depending on campaign scope.
Federation and integration architect	Owns federation trust relationships and integration architecture per Section 8 and 9.	Shared platform, given the cross-agency nature of federation architecture.

◆ 12.2 Common Governance Gaps

- Shared platform governance and individual agency governance are sometimes poorly coordinated, resulting in agency-specific configuration decisions that conflict with shared platform standards.
- Certification campaign ownership is occasionally left ambiguous between the shared platform and individual agencies, resulting in incomplete or inconsistently timed campaigns.
- Service account governance, given the risk pattern identified in Section 11.2, is frequently under-resourced relative to standard workforce identity governance.

XIII. RISK ASSESSMENT AND MITIGATION PLANNING

Multi-agency identity governance programs carry risks distinct from single agency implementations, given the coordination complexity examined throughout this article.

Risk	Likelihood	Impact	Mitigation Approach
Cross-agency mover access not properly revoked	High	High	Implement explicit cross-agency handoff logic per Section 7.2.
SoD rule conflicts between shared and agency-specific rules	Moderate	High	Assign explicit rule ownership per Section 6.2, scoping principle 3.
Certification campaign ownership ambiguity	Moderate to High	Moderate	Assign explicit campaign ownership per Section 12.1.
Dual-platform integration complexity underestimated	Moderate	High	Budget dedicated integration engineering effort per Section 9.2, consideration 3.
Service accounts excluded from standard lifecycle governance	High	Moderate	Establish separate, deliberate service account governance per Section 12.2.

◆ 13.1 Risk Prioritization Guidance

- Cross-agency mover risk should be treated as highest priority given both its high likelihood and its direct connection to the orphaned access and access sprawl findings examined in Section 11.
- SoD rule conflicts and campaign ownership ambiguity are best addressed through the explicit governance role assignments described in Section 12.1, resolved before scaling the platform to additional agencies.
- Integration complexity risk, specific to the dual-platform architecture pattern, should be weighed explicitly during the architecture selection process described in Section 9.2.

XIV. IMPLEMENTATION ROADMAP

Translating this framework into an executable program requires sequencing platform and architecture selection, role modeling, and governance formation.

Phase	Approximate Timeframe	Key Milestones
Architecture Selection	Months 1 to 2	Select an architecture pattern per Section 9.2 based on agency-specific governance and federation priorities.
Role Modeling and Data Collection	Months 2 to 5	Conduct hybrid role modeling per Section 6.1 across initial onboarding agencies.

Lifecycle and Certification Configuration	Months 4 to 8	Configure joiner-mover-leaver workflows per Section 7 and initial certification campaigns per Section 5.
Federation and SoD Rule Implementation	Months 6 to 10	Implement federation architecture per Section 8 and segregation of duties rules per Section 6.2.
Governance Formation and Scaled Onboarding	Months 9 onward	Formalize governance roles per Section 12.1 and onboard remaining agencies using established patterns.

◆ 14.1 Governance Cadence Reference

- **Weekly during active onboarding:** Monitor certification campaign progress and lifecycle event processing.
- **Monthly:** Review risk finding trends per the categories in Section 11 and shared platform configuration compliance.
- **Annually:** Conduct a full identity governance maturity reassessment per Section 10.

XV. CASE PATTERNS AND INDUSTRY BENCHMARKS

This article synthesizes recurring patterns observed across published vendor case material and public sector identity governance research through early 2024, rather than reporting on a single named agency implementation.

Pattern Observed	Reported Association
Dual-platform architecture combining SailPoint governance and ForgeRock federation	More complete governance coverage than either platform's default capability set alone (Section 9.1).
Hybrid role modeling combining bottom-up mining and top-down validation	Faster initial role accuracy than either approach used alone (Section 6.1).
Explicit cross-agency mover handoff logic	Reduced orphaned access findings compared to platforms configured around single-agency assumptions (Section 7.2).
Deliberate, separate service account governance	Improved service account finding reduction relative to the more modest illustrative reduction observed generally (Section 11.2).
Clearly assigned shared versus agency-specific governance roles	Reduced configuration conflicts and campaign ownership ambiguity (Section 12.2).

◆ 15.1 Cross-Program Observations

- **Observation 1:** Multi-agency platforms serving agencies with significant citizen-facing digital service components reported greater relative value from ForgeRock's federation and orchestration strengths, consistent with the consideration described in Section 9.2.
- **Observation 2:** Multi-agency platforms serving agencies under heightened audit and compliance scrutiny, such as those handling federally funded benefit programs, reported greater relative value from SailPoint's certification and governance strengths.
- **Observation 3:** Agencies that treated identity governance maturity progression as a multi-year program, per the roadmap in Section 14, rather than a single implementation project, more consistently reached the higher maturity stages illustrated in Figure 3.

XVI. KEY PERFORMANCE INDICATORS FOR ONGOING GOVERNANCE

Sustaining multi-agency identity governance value requires an ongoing measurement framework spanning provisioning efficiency, certification quality, and risk finding trends.

KPI	Definition	Illustrative Target
Access provisioning time	Average time from access request to fulfillment, benchmarked against Figure 3.	Consistent with or better than the maturity stage the organization has achieved.
Certification campaign completion rate	Percentage of certification campaign items reviewed within the defined campaign window.	High, with minimal items requiring escalation for non-completion.

Certification revocation rate trend	Percentage of certification items resulting in revocation, tracked over time per the governance signal in Section 5.2.	Stable and consistent with actual risk levels, not artificially declining toward zero.
Cross-agency mover incident rate	Number of confirmed cross-agency mover access handoff failures per reporting period.	Low and declining, per the mitigation in Section 13.1.
Risk finding trend by control area	Finding counts by control area, benchmarked against the categories in Table 11.	Declining across all control areas, with particular attention to service account governance.
Identity governance maturity stage progression	Composite score tracked against the five stage model in Section 10.	Steady progression toward higher maturity stages.

XVII. CONCLUSION AND RECOMMENDATIONS

SailPoint and ForgeRock offer complementary rather than directly substitutable capability profiles for multi-agency public sector identity governance, with SailPoint's traditional strength in certification and role governance and ForgeRock's traditional strength in federation and orchestration. Agencies achieve the most complete governance coverage by deliberately architecting around this complementary pattern, whether through a dual-platform architecture or a single platform supplemented by targeted integration, rather than assuming either platform's default capability set alone is sufficient.

◆ 17.1 Summary of Key Findings

- SailPoint and ForgeRock exhibit a consistent complementary strength pattern across the six governance dimensions examined in Section 4, rather than one platform being uniformly superior.
- Cross-agency mover events represent the lifecycle scenario most likely to be mishandled absent deliberate design, directly connected to orphaned access and access sprawl risk findings.
- Provisioning time and risk finding reduction both improve substantially across successive identity governance maturity stages, independent of the specific platform architecture chosen.
- Service account governance remains the risk category showing the smallest illustrative improvement, warranting deliberate, separate governance attention beyond standard workforce identity lifecycle processes.

◆ 17.2 Recommendations

- **Recommendation 1:** Select a deployment architecture pattern deliberately, per Section 9.2, based on the relative importance of governance-intensive versus federation-intensive capability for the specific multi-agency environment.
- **Recommendation 2:** Design explicit cross-agency mover handoff logic rather than relying on default single-agency lifecycle assumptions, per Section 7.2.
- **Recommendation 3:** Assign explicit governance role ownership spanning both shared platform and individual agency responsibilities, per Section 12.1, before scaling to additional agencies.
- **Recommendation 4:** Establish deliberate, separate service account governance rather than assuming standard workforce lifecycle processes adequately cover this risk category.

REFERENCES

- [1] SailPoint Technologies. (2023). "SailPoint IdentityIQ Administration Guide." SailPoint Technical Documentation.
- [2] SailPoint Technologies. (2023). "SailPoint IdentityNow Product Documentation." SailPoint Technical Documentation.
- [3] SailPoint Technologies. (2022). "Identity Security for the Cloud Enterprise." SailPoint Whitepaper.
- [4] ForgeRock. (2023). "ForgeRock Identity Platform Documentation." ForgeRock Technical Documentation.
- [5] ForgeRock. (2022). "ForgeRock Access Management Administration Guide." ForgeRock Technical Documentation.
- [6] ForgeRock. (2022). "Intelligent Access: Orchestrating Authentication Journeys." ForgeRock Whitepaper.
- [7] National Institute of Standards and Technology (NIST). (2020). "Digital Identity Guidelines," NIST Special Publication 800-63-3.
- [8] National Institute of Standards and Technology (NIST). (2019). "Attribute Based Access Control (ABAC) Definition and Considerations," NIST Special Publication 800-162.



- [9] National Institute of Standards and Technology (NIST). (2014, updated 2016). "Guide to Attribute Based Access Control (ABAC) Definition and Considerations." NIST.
- [10] Gartner, Inc. (2023). "Magic Quadrant for Identity Governance and Administration." Gartner Research.
- [11] Gartner, Inc. (2022). "Magic Quadrant for Access Management." Gartner Research.
- [12] KuppingerCole. (2023). "Leadership Compass: Identity Governance and Administration." KuppingerCole Analyst Report.
- [13] National Association of State Chief Information Officers (NASCIO). (2022). "State Identity and Access Management Governance Practices." NASCIO Research Brief.
- [14] American Public Human Services Association (APHSA). (2021). "Shared Services Identity Management Across Human Services Agencies." APHSA Policy Brief.
- [15] Government Technology. (2023). "States Consolidate Identity Governance Across Agencies to Cut Costs and Close Security Gaps." e.Republic Government Technology Publication.
- [16] Internet Engineering Task Force (IETF). (2012). "The OAuth 2.0 Authorization Framework," RFC 6749.
- [17] OpenID Foundation. (2014). "OpenID Connect Core 1.0 Incorporating Errata Set 1." OpenID Foundation Specification.
- [18] OASIS. (2005, with subsequent errata). "Security Assertion Markup Language (SAML) V2.0 Technical Overview." OASIS Standard.
- [19] Ferraiolo, D.F., Kuhn, D.R., & Chandramouli, R. (2007). "Role-Based Access Control," 2nd Edition. Artech House.



INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

 9940 572 462  6381 907 438  ijirset@gmail.com



www.ijirset.com

Scan to save the contact details