KDD098 - External Identity Management

Pending SteerCo Review

Status	Pending SteerCo Review
Owner	HEALY-ext, Michael
Stakeholders	MADASU-ext, Satya

Issue

Syensqo currently utilizes SailPoint & IAS for identity management; however, it has been determined that SailPoint does not align with our long-term strategic vision for managing external (B2B) identities. The business has a rapidly growing footprint of over 30,000 external identities (suppliers and B2B customers). While a centralized, purpose-built platform is the long-term target, current project timelines and resource constraints prevent the immediate deployment of a fully-fledged Identity Governance and Administration (IGA) solution. Consequently, Syensqo lacks a scalable, automated solution and must formally adopt a structured, interim approach to handle the lifecycle and authentication of external partners without blocking future technological integration.

Why a Decision is Required

A formal architectural decision is required to explicitly accept and govern the interim "As-Is" operating model for B2B identity management. Adopting this manual, decentralized approach defers capital expenditure and immediate organizational change, but it requires formal acknowledgment of the compounding operational and security risks. Furthermore, this decision establishes the mandate that current manual processes must be standardized and executed in a way that allows for a seamless retrofit into a centralized IGA solution (such as Microsoft Entra or a capable third-party platform) once resources and timelines permit.

Business and Technical Problems Addressed This decision directly addresses the following immediate realities:

- **Resource and Timeline Feasibility:** Replaces a complex, high-effort IGA deployment with a pragmatic, executable operating model that fits within current resource and timeline boundaries.
- **Strategic Deferment:** Acknowledges the fragmented identity stores (SAP and Salesforce) while intentionally avoiding the creation of custom, point-to-point workarounds that would complicate future modernization.
- **Retrofit Readiness:** Enforces an architecture that establishes the local environments first, keeping the door open for a future overarching identity governance umbrella.

Recommendation

Recommendation: Implement **Option C**—Continue with the Manual Management of External Identities (As-Is) as a formal interim strategy. Supplier identities will continue to be managed manually within SAP Identity Authentication Service (IAS), and B2B customer identities will be managed independently within Salesforce Experience Cloud.

Strategic Rationale Given the strict timelines and limited available resources, attempting to deploy a fully managed IGA service for all external identities is not currently viable. Maintaining the current operating model requires no upfront capital investment and avoids the immediate, cross-functional disruption of a massive data cleanup and architectural re-engineering effort.

Crucially, this approach is designed to be transitional. By operating SAP IAS and Salesforce as distinct, standardized local environments, the organization retains the flexibility to layer a centralized IGA platform over these ecosystems at a later date. This deferred approach accepts short-term operational overhead in exchange for immediate project viability.

Background & Context

Syensqo operates within a complex, multi-tenanted enterprise environment. The organization currently manages over 30,000 external identities—including 15,000 to 20,000 suppliers and thousands of B2B customers—across multiple geographies and business units.

Historically, Syensqo relied on SailPoint Identity Governance as its primary IAM platform. However, SailPoint was architected primarily for internal employee lifecycles and has proven inadequate for the scale and unique requirements of managing B2B external identities.

While the ultimate goal is to move to a unified identity control plane, recent assessments of project timelines and IT resource availability have dictated a phased approach. The organization will temporarily maintain its siloed external identity stores (SAP IAS for suppliers, Salesforce for customers) to ensure business continuity and meet immediate delivery milestones, with the explicit understanding that a centralized identity platform will be retrofitted in a future phase.

Assumptions

1. Technology & Architecture

- **Future Retrofit Viability:** The data structures and manual workflows maintained within SAP IAS and Salesforce will be kept sufficiently standardized to allow for integration into a future IGA platform (e.g., via standard APIs or SCIM) without requiring a complete rebuild of the underlying identity repositories.
- **Siloed Platform Stability:** Both SAP IAS and Salesforce are robust enough to independently handle the anticipated volume of B2B identities without catastrophic performance degradation during the interim period.

2. Organizational & Operational

- **Resource Availability for Manual Operations:** Internal IT, Helpdesk, and administrative teams have the capacity to absorb the linear increase in manual provisioning, deprovisioning, and password reset tickets as the external user base grows.
- **Future Capital Allocation:** Leadership will allocate the necessary budget and resources in a future fiscal cycle to execute the complex data cleanup, mapping, and implementation required for the deferred IGA retrofit.

3. Risk & Compliance

- **Risk Acceptance:** The business formally accepts the increased security and compliance risks inherent in manual identity management (e.g., orphaned accounts, fragmented audit trails) for the duration of this interim phase.
- **Compensating Controls:** Internal audit and security teams will implement manual compensating controls (e.g., periodic spreadsheet-based access reviews) to mitigate the lack of automated governance.

Constraints

1. Operational & Functional Constraints

- **Lack of Automation:** There is no automated trigger or workflow to ensure the timely removal of access when a supplier or customer relationship ends, heavily relying on manual notification from relationship owners.
- **Absence of Self-Service:** Despite native capabilities in the underlying platforms, the current configuration lacks unified self-service, forcing all password resets, attribute updates, and access modifications through internal IT support.

2. Security & Compliance Constraints

- **No Unified Security Baseline:** SAP IAS and Salesforce operate under separate password policies, session management settings, and MFA rules. There is no centralized Conditional Access evaluating external user logins across the estate.
- **Audit Fragmentation:** Evidence of access approvals and account creation must be manually assembled from disjointed emails, IT tickets, and localized system logs, highly complicating compliance attestation.

3. Scalability Constraints

- **Linear Overhead:** With tens of thousands of identities, the manual approach has exhausted practical administrative limits. Business growth will directly correlate with a growing backlog of provisioning tasks or require continuous IT headcount increases.

Impacts

- **Data Quality Degradation:** Manual data entry across multiple systems will inevitably lead to typographical errors, inconsistent naming conventions, and duplicate accounts. This degrades data quality and will significantly increase the complexity of the data mapping effort required for the future IGA retrofit.
- **Orphaned Account Accumulation:** The lack of automated deprovisioning creates a compounding security vulnerability. A material percentage of the 30,000+ external identities will likely become orphaned over time, leaving active credentials exposed.
- **Poor External User Experience:** External partners interacting with multiple Syensqo systems will suffer from password fatigue and disjointed onboarding experiences due to the lack of Single Sign-On (SSO).
- **Opportunity Cost:** Highly skilled SAP and Salesforce administrators will be forced to spend significant time performing routine data entry and helpdesk tasks rather than executing higher-value platform optimizations.

Financial Impact Analysis

1. Immediate Cost Avoidance (CapEx)

- **Zero Upfront Platform Costs:** By deferring the IGA implementation, the organization avoids the immediate capital expenditure associated with purchasing new licensing (e.g., Microsoft Entra MAU billing) and the heavy professional services costs required for a complex deployment.

2. Ongoing & Hidden Operational Costs (OpEx)

- **High Administrative Drain:** The true cost of this model is absorbed into decentralized daily operations. IT administrator hours and helpdesk resources will be consumed by manual account creation, modification, deactivation, and external user password troubleshooting.
- **Audit Preparation Overhead:** The financial cost of internal labour required to manually gather, correlate, and prove compliance across disconnected systems during audit cycles will be substantial.

3. Deferred Technical Debt

- **Future Implementation Premium:** Retrofitting governance onto deeply entrenched, siloed identity stores may cost more than a greenfield deployment. The future IGA implementation may require heavily funded data cleanup effort and complex legacy permission mapping.

Business Rules

To mitigate the risks of this interim manual approach and prepare for the future IGA retrofit, the following rules must be strictly enforced:

1. Strict Identity Segregation

- **Platform Boundaries:** Supplier identities must be managed *exclusively* within SAP IAS. B2B customer identities must be managed *exclusively* within Salesforce. Cross-pollination or manual duplication of identities between these silos without strict business justification is prohibited unless business cases make sense.

2. Data Hygiene & Standardization

- **Standardized Naming Conventions:** All manual account creations must adhere to a strict, globally documented naming and attribute convention. This is critical to ensure identities can be programmatically matched and correlated when the overarching IGA solution is eventually deployed.
- **Mandatory Attributes:** No external account may be created without a valid external email address and a documented internal business sponsor.

3. Compensating Security Controls

- **Manual Access Certifications:** Business unit owners must conduct mandatory, bi-annual manual access reviews. IT will provide user exports from SAP IAS and Salesforce, and business owners must formally sign off on the continued necessity of each external account to mitigate the accumulation of orphaned credentials.
- **Deactivation SLAs:** A strict Service Level Agreement (SLA) must be established requiring relationship owners to notify IT within 48 hours of a supplier contract termination or B2B relationship end, triggering manual deprovisioning.

Options considered

Option A: Microsoft Identity Access Governance

1. Executive Recommendation Implement Microsoft Entra External ID and Entra ID Governance as the centralized identity control plane for all 30,000+ external (B2B) identities. SailPoint will be retained strictly for internal employee governance, establishing a dual-platform architecture.

2. Problem Statement & Context The organization currently manages a rapidly growing base of external identities (partners, vendors, clients) using a mix of SailPoint, manual processes, and point-to-point integrations across SAP and Salesforce. SailPoint is currently architected for internal lifecycles and there are no future plans to use SailPoint for external identities. This fragmentation creates security risks, compliance blind spots, and severe operational bottlenecks for IT.

3. Strategic Rationale

- **Microsoft-First Consolidation:** Natively embeds external identity management within the existing Azure security fabric, extending enterprise protections (like Conditional Access) to B2B users without custom connectors.
- **Scalable "Bring Your Own Identity" (BYOI):** Shifts the authentication burden to the partner's identity provider, drastically reducing helpdesk overhead while maintaining strict logical isolation from the core employee directory.
- **Automated SaaS Provisioning:** Acts as an identity broker, leveraging open standards like SCIM, SAML, and OIDC to automatically provision and revoke downstream access in SAP and Salesforce.

4. Key Assumptions & Constraints

- **Dual-Platform Overhead:** IT and IAM teams must upskill to operate a bifurcated governance model (SailPoint for internal, Entra for external), requiring consolidated reporting for audit purposes.
- **Architectural Nuances:** Native Entra provisioning directly into SAP ERP is unsupported; integrations must be mediated through SAP Cloud Identity Services (IAS). Complex workflows may require custom Azure Logic Apps.
- **Financial Variability:** Microsoft's Monthly Active User (MAU) billing model for guest governance means operational costs will fluctuate month-to-month based on the volume of billable governance events (like access reviews).

5. Mandatory Business Rules & Impacts

- **Strict Segregation:** External users must only reside in Entra (classified as "Guests"), and internal users must only reside in SailPoint.
- **Package-Based, Time-Bound Access:** Direct group or role assignments are prohibited. Access is granted exclusively via Entra Access Packages, which require an internal sponsor and a defined expiration date.
- **Automated Lifecycles:** All downstream provisioning to SAP and Salesforce must be fully automated via Entra. Manual creation or removal of external accounts in downstream systems is forbidden.

Dimension	Assessment	Description

Functional Fit	**High**	Meets core B2B requirements natively, including automated lifecycles, access packages, and BYOI (Bring Your Own Identity) federation. *Caveat: Deeply complex, nested approval workflows may require supplementary custom Azure Logic Apps.*
Strategic Alignment	**High**	Perfectly aligns with the organization's established Microsoft-first cloud strategy. It establishes Azure as the centralized, future-proof identity control plane for external users.
Integration Complexity	**Moderate**	Natively supports open standards (SAML, OIDC, SCIM) for SaaS integration. However, direct SAP ERP provisioning is unsupported and must be mediated through SAP IAS. Salesforce SCIM integrations may also require supplementary internal automation for complex profile mappings.
Ecosystem Alignment	**Excellent**	Consolidates external identity within the existing Microsoft ecosystem. This allows the organization to extend its enterprise security framework (like Conditional Access and continuous threat monitoring) directly to B2B users without requiring complex third-party connectors.
Cost Justification	**Strong (with variability)**	Maximizes ROI on existing Microsoft investments and drastically reduces the hidden operational costs of manual IT provisioning. *Note: The Monthly Active User (MAU) billing model for the Governance add-on introduces month-to-month financial variability that must be actively forecasted.*

Option B: Use SailPoint to Manage All External Identities

Under this option, the organization would leverage its existing SailPoint IdentityNow (or IdentityIQ) deployment to serve as the identity governance and administration (IGA) platform for all external identities. This encompasses both the B2B supplier accounts currently held in SAP IAS and the B2B customer accounts managed within Salesforce.

SailPoint is a mature, market-leading identity governance platform. It provides comprehensive provisioning, access request workflows, certification campaigns, separation-of-duties enforcement, and lifecycle management capabilities. On paper, it comfortably meets the functional requirements for managing external identities.

However, functional capability alone does not make SailPoint the optimal choice for this specific use case. Several material factors—primarily strategic misalignment and architectural complexity—weigh against this option, presenting a compelling case for looking elsewhere.

Functional Assessment

SailPoint can natively fulfil the core requirements of external identity management:

- Automated provisioning and deprovisioning of external user accounts across target systems.
- Access request and approval workflows for external user onboarding.
- Access certification campaigns to periodically review and attest external user entitlements.
- Policy enforcement, including separation of duties and role-based access control.
- Audit logging and reporting for compliance and governance purposes.

In isolation, these capabilities make SailPoint a highly credible candidate. The challenge lies not in what SailPoint can do, but in whether it is the right strategic investment for the organization's future state.

Strategic Misalignment

SailPoint is not positioned as the strategic IAM solution for this organization. The business has already established its direction of travel toward the Microsoft Entra platform as the primary identity provider and governance layer. This strategic decision reflects the organization’s deep investment in the Microsoft ecosystem across infrastructure, productivity, security, and cloud services.

Selecting SailPoint for external identity management would run directly counter to this strategic direction. It requires committing further budget, skills, and operational capacity to a platform that is not the long-term strategic focus. Every pound spent on SailPoint licensing, advanced configuration, and specialist resources is a pound diverted away from the platform that will form the backbone of the organization’s future identity architecture.

From an architectural governance perspective, introducing SailPoint as the external identity layer alongside Microsoft Entra for internal identities creates a dual-platform IAM landscape. This increases architectural complexity, requires maintaining two sets of operational expertise, and fragments the enterprise identity management narrative.

Integration Complexity (Multi-Vendor Landscape)

SailPoint does offer supported, out-of-the-box connectors for both target platforms:

- **SAP IAS:** SailPoint provides a standard SAP Cloud Identity Services integration capable of managing users and groups within SAP IAS.
- **Salesforce:** The standard SailPoint Salesforce connector natively supports the management of external Community and Experience Cloud users, including profile and permission set assignments.

However, the availability of these connectors does not eliminate the implementation burden. Leveraging them still introduces significant integration challenges:

- **Advanced Configuration:** While ground-up coding is not required, mapping complex external user attributes and business logic between SAP, Salesforce, and SailPoint requires specialized SailPoint engineering expertise.
- **Vendor Dependency:** The organization remains at the mercy of three different vendors (SailPoint, SAP, and Salesforce) for API updates, connector patching, and version compatibility.
- **Operational Silos:** Managing external identities in SailPoint while managing internal identities in Entra ID prevents the organization from establishing a unified, single-pane-of-glass view for enterprise-wide access routing and identity risk.

Ecosystem and Vendor Alignment

The organization operates heavily within a Microsoft environment, built on Azure, Microsoft 365, and the broader Microsoft security and identity stack. Microsoft Entra ID already serves as the identity provider for the internal workforce. Choosing SailPoint for external identities introduces a competing governance platform that does not natively benefit from the shared security context, telemetry, and unified management plane provided by the Microsoft ecosystem.

By contrast, an Entra-centric approach allows for native integration with the tools already managing internal identities, Conditional Access policies, security monitoring, and compliance. Selecting SailPoint forfeits these consolidation advantages.

Cost Considerations

The total cost of ownership (TCO) for the SailPoint option extends well beyond basic platform capability:

- SailPoint platform licensing (per-identity or subscription model for external users).
- Specialist SailPoint engineering resources (internal or contracted) for advanced connector configuration and business logic mapping.
- Ongoing operational overhead to maintain a secondary identity platform.
- The opportunity cost of investing in a non-strategic platform instead of consolidating on Microsoft Entra.

When these costs are aggregated and compared against the investment required for a Microsoft-native solution—which benefits from existing licensing agreements, native ecosystem integration, and familiar tooling—the SailPoint option becomes difficult to justify financially.

Summary Assessment: Option B

Dimension	Assessment
Functional Fit	**High.** Meets all core external identity management requirements including provisioning, lifecycle management, access governance, and certification campaigns.
Strategic Alignment	**Low.** SailPoint is not positioned as the strategic IAM platform for the organization. Investment here runs counter to the established direction toward Microsoft Entra.
Integration Complexity	**Moderate to High.** While out-of-the-box connectors exist for SAP IAS and Salesforce, configuring them to handle complex B2B lifecycle logic across a multi-vendor landscape requires niche expertise and increases architectural debt.
Ecosystem Alignment	**Poor.** The organization is invested in the Microsoft stack. Introducing SailPoint creates a parallel IAM ecosystem, increasing complexity and operational overhead.
Cost Justification	**Difficult to justify.** Licensing, specialist SailPoint skills, and parallel platform maintenance represent a significant investment in a technology outside the long-term IAM strategy.

Option C: Decentralized Management with API Improvements (No IGA)

Under this option, the organization adopts a decentralized but highly optimized operating model. By prioritizing native platform capabilities and modern API integrations, the business drives immediate onboarding efficiencies across both external ecosystems. This approach modernizes both SAP Identity Authentication Service (IAS) and Salesforce Experience Cloud independently, achieving operational gains without much upfront capital investment or organizational change management required to deploy a centralized Identity Governance and Administration (IGA) platform.

While SAP IAS and Salesforce will continue to operate as fragmented identity stores, this approach delivers tangible, value improvements to both supplier and B2B customer onboarding processes.

Preserving Future Flexibility

Managing SAP and Salesforce locally inherently creates a decentralized architecture, but it strategically preserves options for the future. By establishing mature, automated local environments first, the organization effectively lays the groundwork for a future overarching governance implementation. If the business decides to introduce an enterprise-wide IGA solution later, the local automation and delegated structures established within these platforms will already be functioning efficiently. Future integrations become a matter of applying central oversight to processes that are already technically optimized.

Operating Model (Target State): SAP IAS

This approach shifts the organization away from manual administration for its 15,000 to 20,000 external suppliers, introducing an automated, self-service-oriented model:

- **Automated Provisioning:** Supplier creation is triggered directly from SAP S/4HANA via the SAP Cloud Identity Services API, entirely removing the need for manual user creation by internal SAP Security administrators.
- **Empowered Delegated Administration:** Upon creation, an automated email empowers a designated external Supplier Administrator. By logging into IAS, these admins take ownership of onboarding, managing, and maintaining their own users, effectively crowdsourcing the administrative effort.
- **Federated SSO:** Supplier Admins gain the flexibility to request federated Single Sign-On (SSO) to integrate their own corporate credentials.
- **Automated Access Management:** IAS APIs are leveraged to dynamically apply IAS Groups for user access, removing routine enforcement tasks from internal IT.

SAP IAS Advantages and Disadvantages

Advantages:

- **Scalability:** Reduces internal IT bottlenecks, allowing supplier onboarding to scale seamlessly with business growth.
- **Partner Autonomy:** Improves the partner experience by giving them direct control over their own workforce's access without waiting on IT helpdesk tickets.
- **Process Velocity:** Automated triggers from S/4HANA ensure that access is provisioned the moment a supplier contract is finalized in the ERP.

Disadvantages:

- **The "Orphaned Account" Risk:** The delegated model relies entirely on external Supplier Admins to promptly deactivate users who leave their company. Without central oversight, this creates a high risk of active credentials lingering indefinitely.
- **Audit Blind Spots:** Gathering evidence for compliance audits (e.g., proving who approved a specific user's access) is difficult when administration is delegated externally without an overarching governance logging tool.
- **Extra Tenant Needed**: A new IAs tenant will need to be procured to ensure all external ID's are held in the IAS tenant. Additional cost to ensure no mixture of Internal & external ID's

Operating Model (Target State): Salesforce

Moving away from the legacy approach of email-driven or spreadsheet-initiated provisioning, the organization will implement native Salesforce automation to handle thousands of B2B customer identities:

- **Automated Self-Registration:** Utilizing Salesforce Flow Builder, the organization will expose intelligent self-registration pages. These flows automatically match registrant email domains to existing B2B Accounts and route approval requests to the appropriate internal account owner.
- **Just-in-Time (JIT) Provisioning:** For larger B2B clients utilizing federated SSO, Salesforce will intercept SAML assertions via JIT Provisioning to automatically create user records and assign permissions on the fly during their first login.
- **Delegated External Administration:** Similar to the SAP model, designated "Super Users" at client organizations will be granted external delegated admin rights to manage their own colleagues within the Experience Cloud portal.

Salesforce Advantages and Disadvantages

Advantages:

- **Frictionless Customer Experience:** JIT provisioning and automated self-registration ensure customers can access portals, catalogs, and support immediately, enhancing brand perception.
- **Contextual Access:** By leveraging Salesforce User Access Policies, permissions are automatically tied to the user's CRM data (e.g., tier, region, purchased products), ensuring highly accurate, dynamic entitlement mapping.
- **Reduced Support Costs:** Shifting routine password resets and user creation to customer "Super Users" drastically lowers ongoing operational costs.

Disadvantages:

- **Data Silos and Duplication:** Because Salesforce and SAP remain disconnected, an external user who acts as both a supplier and a B2B customer will have two entirely separate identities, requiring them to manage two profiles.
- **Inconsistent Security Posture:** Internal IT must manually dual-maintain security policies. If the organization decides to mandate a new Multi-Factor Authentication (MFA) requirement, it must be configured, tested, and deployed twice—once in Salesforce and once in SAP IAS.

Considerations and Inherent Risks of Decentralization

While the API improvements deliver excellent operational efficiency, maintaining a decentralized architecture does introduce certain visibility and governance trade-offs. Relying on fragmented systems means that cross-platform reporting and unified lifecycle management require more manual coordination.

Summary of Risks: Option C

Risk Category	Impact of Continuing Manual Management
Data Consistency	Empowering external Supplier Admins (SAP) alongside manual internal entry (Salesforce) can lead to varied attribute formats and naming conventions, which may require data cleanup if an IGA platform is introduced later.
Account Lifecycle Management	The delegated model relies heavily on external Supplier Admins to promptly deactivate departing users. Without automated, centralized HR/contract cross-referencing, there is an increased chance of inactive accounts remaining enabled longer than necessary.
Audit & Visibility	Delegated administration without a central overarching dashboard means that gathering audit evidence—such as who approved access or periodic access reviews—requires compiling logs manually across multiple distinct systems.
Scalability of Oversight	While the *provisioning* bottleneck is solved via API, the effort required by internal compliance teams to audit and monitor the actions of thousands of external SAP Supplier Admins will increase as the partner ecosystem grows.
Policy Alignment	Operating independent identity stores requires internal IT to manually dual-maintain security policies (like password complexity and MFA requirements) to ensure a consistent security posture across the enterprise

Evaluation

Option A

Decision Parameter	Pros ⊕	Cons ⊖	Overall Assessment
Feasibility & Functional Fit	• Purpose-built for external scale (30,000+ users). • Natively supports BYOI (Bring Your Own Identity), automated lifecycles, and access packages.	• Deeply nested or highly customized legacy approval workflows may require supplementary custom Azure Logic Apps.	**High.** Highly capable of handling the current and future external identity scale natively, replacing error-prone manual steps with automated enforcement.
Complexity (Architecture & Integration)	• Centralizes external identities within the existing Azure fabric. • Out-of-the-box SCIM support for downstream applications like Salesforce.	• Based on the current set up, this would Establish a dual-platform architecture (SailPoint internally, Entra externally)	**Moderate.** Consolidation drastically simplifies the Microsoft estate, though downstream SaaS integrations and dual-platform operations introduce specific technical nuances.
Cost & Effort to Implement	• Maximizes ROI on the organization's existing Microsoft cloud investments. • Delivers massive long-term reduction in IT helpdesk costs through self-service and automation.	• Requires upfront effort for data cleansing, extraction, and platform configuration. • Monthly Active User (MAU) billing for guest governance introduces month-to-month financial variability.	**Strong ROI.** The upfront implementation effort and training are heavily offset by significant long-term operational savings, automated compliance, and risk reduction.
Ongoing Operational Impact & Cost	• Drastically reduces manual provisioning tickets. • Shifts the authentication and credential management burden to external partners.	• Requires the IAM team to upskill and maintain dual-platform competency + Additional headcount will be needed to support this • Managing complex access packages may remain an IT task due to UI limitations for business users.	**Net Positive.** Replaces manual administrative busywork with automated governance, transforming the IAM team's role from execution to oversight.
Program Principles & Deviations	• Strictly aligns with Zero Trust, least privilege, and Microsoft-first consolidation principles. • Guarantees an auditable, single source of truth for external access.	• *Deviation:* Abandons the "single IAM tool for everything" concept by establishing a specialized B2B boundary separate from the internal SailPoint platform.	**Strong Alignment.** The architectural deviation of a dual-platform model is a strategic necessity to achieve enterprise-grade B2B security and scalability.

Option B

Decision Parameter	Pros ⊕	Cons ⊖	Overall Assessment
Feasibility & Functional Fit	• High functional maturity. • Natively handles provisioning, governance, and access workflows. • Out-of-the-box connectors for SAP IAS and Salesforce exist.	• Feasibility drops when factoring in the required niche SailPoint engineering skills to map complex B2B logic.	**Moderate.** Functionally feasible on paper, but practically hampered by the need for highly specialized configuration outside the organization's core skill set.
Complexity (Architecture & Integration)	• Standard vendor connectors provide a baseline starting point.	• Introduces a dual-platform IAM landscape alongside Entra. • Tri-vendor dependency (SailPoint, SAP, Salesforce) for API updates and patching.	**High Complexity.** Increases architectural debt and fragments the identity ecosystem, preventing a unified security posture.
Cost & Effort to Implement	• Prevents the need for ground-up custom connector coding.	• High upfront licensing costs for external users. • Premium rates for specialized SailPoint implementation engineers. • High opportunity cost (diverting funds from the strategic Microsoft roadmap).	**High Cost/Effort.** Difficult to justify the capital expenditure when the organization is already heavily invested in Microsoft entitlements.
Ongoing Operational Impact & Cost	• Strong audit logging and compliance reporting capabilities.	• Creates operational silos; requires maintaining two sets of administrative expertise. • Forfeits native consolidation benefits of the Microsoft stack (e.g., shared telemetry, unified Conditional Access).	**High Negative Impact.** Splitting internal (Entra) and external (SailPoint) identities prevents a single-pane-of-glass view of enterprise access and risk.

Program Principles & Deviations	• Meets baseline security and governance compliance principles.	• **Major Deviation:** Directly contradicts the established strategic principle of utilizing Microsoft Entra as the primary identity provider. • Violates consolidation and simplification principles.	**Critical Failure.** Selecting SailPoint actively works against the organization's stated architectural direction and cloud strategy.

Option C

Decision Parameter	Pros	Cons	Overall Assessment
Feasibility & Functional Fit	• Leverages existing SAP Cloud Identity Services APIs to automate provisioning from S/4HANA. • Utilizes native Salesforce tools (Flows, JIT) for automated B2B onboarding. • Empowers partners and customers via delegated administration and federated SSO across both platforms. • Leaves the architecture open for a future IGA retrofit without vendor lock-in today.	• Lacks centralized cross-system lifecycle management. • Relies heavily on external admins to promptly deprovision users in *both* systems, which can lead to lingering active accounts across the digital estate.	**High (Locally).** Functionally excellent for immediate onboarding needs and external self-service across both SAP and Salesforce, though it entirely lacks an enterprise-wide governance layer.
Complexity (Architecture & Integration)	• Capitalizes on successful API integrations and native platform capabilities rather than requiring a net-new enterprise architecture. • Defers the complex design decisions and heavy lift of deploying a full centralized governance platform.	• Fragmented architecture means a "single pane of glass" for identity visibility does not exist natively. • Retrofitting an IGA later will require mapping delegated permissions and normalizing data across two distinct, highly customized silos.	**Moderate.** Technical complexity is effectively contained to platform-specific workflows, keeping the overarching architecture lean, though cross-system governance remains a manual challenge.
Cost & Effort to Implement	• Maximizes ROI on recent SAP integration work and existing Salesforce licenses. • Avoids significant upfront licensing, deployment costs, and organizational change management associated with a new governance tool.	• Requires upfront configuration effort to build and test Salesforce automations. • Gathering cross-system audit evidence remains a labor-intensive manual effort. • Future IGA integration will carry compounded data consolidation costs.	**Cost-Effective (Short-Term).** Highly efficient use of current investments, delivering immediate value to both SAP and Salesforce workflows while deferring overarching governance expenses.
Ongoing Operational Impact & Cost	• Drastically reduces internal IT workloads across both SAP and Salesforce through automated provisioning and delegated administration. • Significantly improves the external user experience via self-service and flexible authentication options.	• Internal compliance and security teams face a multiplied manual effort to audit the actions of external admins across two separate, disconnected systems.	**Net Positive for IT Operations.** Provides massive operational relief for internal identity and support teams, though it shifts a heavy, manual burden onto audit and compliance functions.
Program Principles & Deviations	• Strongly aligns with principles of automation, self-service, and process efficiency within the local ecosystems. • Retains strategic flexibility for future platform decisions.	• **Deviation:** Departs from the principle of centralized governance and unified visibility. • Security posture (MFA, session policies) must be manually dual-maintained across independent platforms.	**Partial Alignment.** Successfully achieves local automation and operational efficiency, but defers holistic enterprise identity consolidation and oversight.

See also

File	Modified
PDF File Endorsement - Thierry Ma.pdf	Apr 21, 2026 by WENNINGER-ext, Sascha
PDF File Endorsement - Michael Pacaud.pdf	Apr 21, 2026 by WENNINGER-ext, Sascha
PDF File Endorsement - Thierry Ma - additional context.pdf	Apr 21, 2026 by WENNINGER-ext, Sascha

Download All

Change log

Version	Published	Changed By	Comment
CURRENT (v. 20)	**Apr 08, 2026 10:07**	**WENNINGER-ext, Sascha**	
v. 19	Mar 25, 2026 21:18	**HEALY-ext, Michael**	
v. 18	Mar 25, 2026 21:14	**HEALY-ext, Michael**	
v. 17	Mar 25, 2026 21:08	**HEALY-ext, Michael**	
v. 16	Mar 25, 2026 20:59	**HEALY-ext, Michael**	
v. 15	Mar 25, 2026 20:58	**HEALY-ext, Michael**	
v. 14	Mar 24, 2026 12:40	**HEALY-ext, Michael**	
v. 13	Mar 24, 2026 12:38	**HEALY-ext, Michael**	
v. 12	Mar 24, 2026 10:16	**HEALY-ext, Michael**	
v. 11	Mar 23, 2026 11:10	**HEALY-ext, Michael**	

Go to Page History

Workflow history

This view shows the 5 most recent entries. The complete workflow log is available from the 'Document Activity' menu item.

Apr 21, 2026	Actor	Type	Activity	Version
Pending SteerCo Review	WENNINGER-ext, Sascha	State	changed expiry date to '05 May, 2026 08:01 am' at 8:01 am	
		State	changed state to Pending SteerCo Review at 8:01 am	v20
Pending Stakeholder Review	WENNINGER-ext, Sascha	State	gave *Stakeholder Review* approval at 8:01 am *Endorsed by Thierry Ma and Michael Pacaud*	
Apr 09, 2026				
	WONG-ext, Oliver	State	changed expiry date to '16 Apr, 2026 10:31 am' at 10:31 am	
		State	changed state to Pending Stakeholder Review at 10:31 am	v20
Pending Design Authority Review	WONG-ext, Oliver	State	gave *Design Authority Endorsement* approval at 10:31 am *DA Endorsed*	
Apr 08, 2026				
	WENNINGER-ext, Sascha	Edit	updated the page at 10:07 am	