kuppingercole ANALYSTS

Commissioned by:

ROIABLE

Navigating SAP IdM End-of-Maintenance: Evaluating Migration Options

Nitish Deshpande

December 2, 2025

This KuppingerCole Whitepaper dives deeper into the complexities that could arise from organizations moving away from SAP Identity Management (IdM) to Microsoft Entra or other IAM solutions. The migration poses a significant challenge and organizations need to take steps sooner rather than later. A technical overview of ROIABLE's ROI intelligent Access Management (ROI iAM) portfolio as an accelerator for assessment, phased migration, and integration with enterprise governance and access control solutions is included in this report.

Contents

Figures

Introduction

SAP's announcement that SAP Identity Management (IdM) 8.0 will reach end-of-maintenance in 2030 has created unexpected urgency for approximately 2000-3000 organizations worldwide. Unlike typical product transitions, SAP IdM environments are deeply embedded in the SAP landscape and often comprising a number of custom connectors, hundreds of processes, and often complex integrations with SAP GRC Access Control and other non-SAP systems.

The migration from SAP IdM involves navigating complex legacy system architectures comprised of interconnected components, each requiring careful analysis. A successful transition requires thorough audits to identify which elements can transition smoothly and which will require new configurations. This process demands tooling capable of delivering deep insights into the current IT landscape to support informed, strategic decisions.

A key task in migration preparation consists of evaluating current identity infrastructures and processes. This involves detailed assessments of asset usage and the wider implications on governance, risk, and compliance. Leveraging advanced analytical tools is required for ensuring a smooth transition that covers all components of identity management systems.

To minimize disruption, thorough planning and execution are required from initial audits to implementing the new solution(s). Real-time data and automation provide valuable insights into asset utilization and facilitate efficient resource allocation during the migration process.

Target architectures vary. Some organizations will adopt Microsoft Entra as the leading IAM, others will choose another dedicated IGA platform. Either way, the migration approach should be modular: discover and estimate, introduce a sidecar for new provisioning, migrate connectors stepwise, maintain or extend risk analysis, and then decommission SAP IdM only when business processes, attestations, and audit trails are retained.

In this context, vendors like ROIABLE offer essential support by providing tailored solutions and strategic tooling for organizations navigating this migration. Apart from the main product – ROI iAM, ROIABLE is offers several additional tools and services integrated with the main product for further streamlining the migration process. This includes an SAP IdM Migration Analyzer, an SAP GRC risk analysis and provisioning accelerator and an MS Entra provisioning accelerator. These solutions are designed to accelerate assessment, maintain GRC posture, and enable an event-driven architecture across the solutions. Further insights into ROIABLE’s methodologies will be explored in the Vendor Spotlight section of this whitepaper.

Highlights

- SAP IdM 8.0 environments typically contain 40-60% unused or obsolete objects; automated analysis is essential before migration planning
- Organizations maintaining SAP GRC Access Control can preserve their SoD policies through proxy integration patterns during migration

- Event-driven sidecar architectures enable phased migration without disrupting active provisioning flows
- Microsoft Entra ID requires SAP-specific extensions to handle authorization structures; gap-filling accelerators reduce custom development significantly.
- Migration programs without detailed asset inventories experience 3-4x budget overruns and timeline delays

Overview

Most SAP IdM environments involved teams implementing custom connectors, writing scripts, and assembled processes to fit business needs. Over time, those objects piled up. The first step in migration is to measure what exists and what is used. A good analyser should compare original packages with the current state, categorize objects such as original, modified, new, or custom, and produce reports on processes, forms, entry types, and attributes. This should be done ideally with counts of used versus unused. That distinction helps prioritization as only the used and business-critical pieces need to be migrated or redesigned.

Common Migration Pitfalls

Organizations should take the below three things in consideration when approaching SAP IdM migration:

1) Single phase migration: Attempting to switch all systems simultaneously (as a big bang) creates unnecessary risk
2) GRC abandonment: Discarding SAP GRC Access Control forces rebuilding SoD rules from scratch and sometimes losing important SAP context.
3) Premature decommissioning: Disconnecting SAP IdM before establishing another centralized source of truth.

Configuration analysis alone is insufficient. Organizations must also inventory active versus dormant objects, as research shows that 40-60% of custom SAP IdM scripts are no longer invoked in production environments. Estimation jobs that scan scripts, tasks, and jobs provide concrete numbers for each identity store and package. For instance, an analyzer might report: '847 total processes, 312 original SAP-delivered, 198 modified, 337 custom. Of these, 156 processes show zero executions in the past 12 months.'

While the discovery is running, setting up a safe staging area for new integrations is recommended. An event-driven sidecar allows teams to migrate or create new connectors one by one. The sidecar accepts REST events from the leading IAM, translates them to the native interfaces of SAP and non-SAP targets, and feeds results back asynchronously. System for Cross-domain Identity Management (SCIM) can be exposed to the leading IAM for a standards-based provisioning, while the sidecar connects downstream to SAP BTP services, SAP Integration Suite connectors, or other protocols.

Many organizations rely on SAP GRC Access Control for SoD analysis, risk-aware approvals, and policy enforcement. The migration architecture should treat SAP GRC as the

place where access requests are evaluated and approved, while using a proxy to extend GRC's reach to non-SAP targets, including roles and permissions. This ensures cross-system risk analysis throughout the migration.

Organizations choosing Microsoft Entra as the leading IAM may face functional gaps for SAP-specific scenarios. A provisioning accelerator closes these gaps by providing prebuilt event processing, mapping, and callback patterns. It lets Entra orchestrate onboarding, approvals, and provisioning while an SAP-aware sidecar handles SAP authorization structures, risk analysis requests, and maintains consistency back to the leading IAM.

Rewinding 10 years back the self-service of SAP IdM was not the state-of-the-art solution, which one could expect from a modern IAM. User interfaces age quickly and require frequent redevelopment, which is inefficient for organizations with evolving requirements. To address this, ROIABLE uses SAP Joule AI. With natural language input, users can review their current access and request new access while following the required approval and compliance steps.

However, there are several technical and operation points that need to be taken into consideration when performing the migration. These considerations are further highlighted in the upcoming segments of this whitepaper.

Technical Considerations for Migration

A successful SAP IdM migration balances four obligations: continuity of provisioning, continuity of governance, preservation of evidence, and measurable reduction of technical debt.

Technical Architecture Decisions

Organizations face three primary architectural choices:

Approach	Environment	Risks
Direct replacement	Simple environments (<50 connectors), single SAP landscape	Loss of SAP-specific capabilities
Sidecar pattern	Complex environments with SAP GRC dependency	Additional integration point to maintain
Dual-stack interim	High-risk environments requiring parallel validation	Increased operational overhead

Continuity of provisioning

Identity lifecycle events such as joiner, mover, leaver must continue to trigger account creation, role assignment, and deprovisioning across SAP and non-SAP systems. Event-driven integration requires REST endpoint capabilities in the leading IAM, asynchronous callback handling, and error queuing. Organizations using Microsoft Entra ID must verify that their E3/E5 licensing includes lifecycle workflows and custom extensions. SCIM provides the resource model for identities, groups, and entitlements. The sidecar translates these into target-specific operations through SAP Integration Suite connectors, which cover all major systems and protocols.

Continuity of governance

Approvals, SoD checks, and access certifications cannot be interrupted. Where SAP Access Control is in place, connect the sidecar so that GRC can continue to receive requests for risk analysis. The sidecar should understand SAP authorization structures and convert target objects into the standard shape GRC expects. For non-SAP systems, it should register objects in a way GRC can analyze, enabling cross-system risk analysis and policy enforcement from a single GRC cockpit.

Preservation of evidence

The side-by-side design acknowledges SAP IdM as the interim audit repository. It keeps hollow structures synchronized so that requests, approvals, and provisioning outcomes are recorded centrally until final decommissioning which is important for audit purposes. When the organization is ready, switch the authoritative audit source to the new stack and SAP IdM databases can be archived appropriately.

Reduction of technical debt

Migration forces inventory of unused packages. Organizations typically eliminate 40-60% of custom objects during migration. The SAP IdM Migration Analyzer by ROIABLE reports that split objects into original, modified, new, and custom, used and unused make it easy to remove the unnecessary objects during migration. Estimation outputs quantify process and script churn per package, helping teams decide what to redesign versus replace with out-of-the-box capabilities in the target environment

Data model translation

SAP IdM customers often embedded business logic and custom events into entry types and attributes. The migration should either (a) preserve semantics by moving to attributes and access packages in the leading IAM, or (b) externalize business logic to the sidecar’s mapping layer. The analyzer’s reports on attributes, entry types, and their usage become the blueprint for this translation

Cutover governance

When disconnecting SAP IdM, ensure all approval processes live in the leading IAM or GRC, all provisioning flows have passed operational SLAs, reporting shows parity or improvement and audit packages capture before/after evidence. The final state should document decommissioning and data archiving for compliance

Operational Considerations for Migration

Migrating from SAP IdM involves addressing several critical requirements to ensure a seamless and successful transition. The process involves a comprehensive and robust audit of the existing identity management infrastructure. This audit involves a detailed examination of current configurations, dependencies, and the roles within the existing setup. It is essential to determine which components of the SAP IdM system can integrate seamlessly with new IAM platforms and which aspects require reconfiguration or a complete overhaul.

Audit and Inventory

The foundation of an effective migration strategy is a thorough audit of the existing identity management infrastructure. This audit involves examining current configurations, dependencies, and roles within the existing setup. Organizations must determine which components of the SAP IdM system can integrate with new IAM platforms and which require reconfiguration or complete overhaul. Developing an inventory of identity assets forms the basis for understanding the scope of migration and resource allocation.

Compliance and Security Alignment

Ensuring compliance with data protection regulations and security standards remains an important aspect of the migration process. Integration of advanced security features, including risk management and auditing capabilities, to protect identity data and meet compliance requirements.

SAP IdM-Specific Stakeholder Alignment

Unlike typical IAM projects, SAP IdM migration requires engagement across organizational boundaries:

- SAP Basis teams (who own the NetWeaver platform and the database layer)
- SAP GRC administrators (who maintain SoD rule sets)
- Custom development teams (who built connectors and processes)
- Audit and compliance (who rely on SAP IdM as system of record)

The most critical alignment occurs with GRC teams: determine early whether SAP Access Control will remain the authoritative SoD engine or whether policies will be migrated to the new platform. With the sidecar running in the cloud, the option of retaining existing SAP GRC setup becomes the easy to choose option.

Technical and Operation Continuity

Maintaining continuity during the migration process requires that existing and new systems operate in parallel alongside legacy infrastructure temporarily. Preparation of contingency plans to address potential disruptions and ensure swift recovery in case of unforeseen challenges.

Addressing these key requirements necessitates a structured approach, detailed planning, and expert execution. Meanwhile, utilizing advanced analytical tools provides the necessary insights to develop effective strategies, empowering organizations to navigate migration challenges efficiently. Ensuring compliance, aligning stakeholder engagement, and maintaining operational continuity are integral to a successful SAP IdM migration, laying the groundwork for an optimized identity management ecosystem.

Migration Methodology

The process of SAP IdM migration begins with a detailed analysis of existing systems. This involves establishing a comprehensive inventory of all identity-related assets and dependencies.

Define the Target Operating Model (TOM)

Decide the leading IAM (e.g., Entra or other IGA platform) and define responsibilities between the leading IAM, SAP GRC, and the sidecar. In the TOM, the leading IAM handles application onboarding, lifecycle events, and user-facing approvals; the sidecar handles mappings, provisioning, and callbacks; SAP GRC performs risk analysis and enterprise approvals where required.

Total Cost of Ownership Factors

Migration costs extend beyond tool licensing:

- SAP BTP consumption: SAP Integration Suite and its Event Mesh feature, as well as SAP HANA Cloud database service incur usage-based charges
- Parallel licensing: SAP IdM can be moved to the cloud via the sidecar without committing to a new IAM platform licenses. Customers purchase leading IAM licenses only when ready to transition, and the selected platform then connects to ROI iAM.
- Professional services: Partner implementation effort

Organizations should model TCO across the full migration timeline, not just first-year costs.

Migration Timeline Expectations

Based on KuppingerCole analysis of similar migrations:

- Small environments (1,000-5,000 identities): 9-12 months
- Mid-sized (5,000-25,000 identities): 12-18 months

- Enterprise (>25,000 identities): 18-30 months

These timelines assume dedicated resources and executive sponsorship. Organizations attempting migration with existing IAM team capacity should add 40-60% to these estimates.

Side-by-side architecture

Deploy the sidecar on SAP BTP; connect to SAP Integration Suite for connectors and event mesh; configure SCIM to the leading IAM; and enable proxy registration in SAP IdM for audit shadowing. Begin routing new systems through the sidecar while leaving existing SAP IdM integrations untouched

Migrate sources and identities

Connect HR and company data sources to the sidecar with daily load jobs. Validate identity joins and attribute mappings end-to-end and sample access package requests in the leading IAM. Ensure event flows and SCIM payloads align with identity lifecycle policies

Migrate high-value targets in phases

For SAP targets (e.g., S/4HANA, IAS/IPS), configure connector flows in SAP Integration Suite; expose SAP authorization structures to GRC via the sidecar; and complete risk analysis before provisioning. For non-SAP SaaS, register entitlements and route approvals either natively in the leading IAM or via GRC if SoD is in scope. Reconcile before cutover and track incidents with dashboards

Extend GRC to non-SAP systems

Use the sidecar to onboard non-SAP targets into SAP GRC for risk analysis. The accelerator pattern minimizes changes to the existing GRC logic while enabling cross-system SoD analysis and approvals. This preserves the enterprise compliance posture throughout migration

Redesign approvals and user experience

Move identity lifecycle and access request interfaces to the leading IAM. Where Entra is selected, leverage its workflows and access packages; supplement with event-based callbacks and app roles for SAP-aware provisioning. Validate that manager and application owner approvals remain clear and auditable

Certify and report

Run access review campaigns using reporting dashboards; verify anomaly rates and orphaned accounts; and export evidence to Excel for auditors. Monitor reconciliation drift and remediation times as success metrics for each cutover wave

Monitoring and evaluation

These are continuous processes in migration projects. Businesses must regularly refine their identity management strategies, employing ROIABLE's historical analytical insights to adjust processes and governance structures dynamically. Such adaptability is key in maintaining a strategic advantage in identity management practices.

Scenarios Where Alternative Approaches May Be Preferable

The sidecar/proxy pattern described in this whitepaper covers a lot of use cases, but organizations might want to consider also other alternatives when:

- SAP IdM implementation is not heavily customized and organizations are not looking for real migration of the technical artefacts, rather more a business shift to the newly selected IAM. In this case a direct replacement with another leading IAM using big bang might be a more suitable approach
- Organizations are abandoning SAP GRC Access Control for another solution and integrating the replacement in the sidecar is a cumbersome task: Consider connecting the replacement solution directly to an IAM that has a connector out of the box
- Organizations have not onboarded the SAP Business Technology Platform and are not yet using any services running on it (e.g. SAP Integration Suite): The sidecar is running completely in SAP BTP and relying on the existence of certain services. Probably onboarding the platform just for this particular case won't be financially efficient and we would recommend to search for other alternatives

In summary ROI iAM is very well positioned for customers looking to move away from SAP IdM, which might or might not have an SAP GRC connection and have already adopted the SAP Business Technology Platform with some of its underlying core services.

Migration Completion Criteria

SAP IdM can be decommissioned only when:

- All identity lifecycle events (joiner/mover/leaver) execute successfully through the new platform for 30+ consecutive days
- Access certification campaigns complete with <5% error rate
- SoD violations are detected and blocked at provisioning time
- Audit queries can be satisfied from new system logs
- No active SAP IdM pending requests or process instances
- Database exports are archived per compliance retention requirements

ROIABLE – ROI iAM

ROIABLE is an SAP partner with deep SAP IdM expertise. The company offers targeted products aimed at SAP IdM customers who want to migrate while maintaining governance and minimizing re-engineering. The ROI iAM portfolio includes an SAP IdM Migration

Analyzer, an SAP GRC risk analysis and provisioning accelerator, and a provisioning accelerator for Microsoft Entra. These components together enable evidence-based planning, side-by-side migration, and sustained risk management across SAP and non-SAP estates.

ROIABLE structures implementation timelines based on landscape complexity rather than the number of identities, while licensing drives size from a identity-count perspective.

- Small environments typically involve SAP-centric landscapes with up to 50 production systems and standardized processes and are completed in 6 to 9 months.
- Medium environments expand to include integrated SAP GRC, two to three custom connectors, and up to 100 production systems, resulting in timelines of 9 to 12 months.
- Large environments may use any leading IAG platform, including multiple custom connectors, customized processes, and up to 250 production systems, with implementation durations ranging from 12 to 24 months.

Market Positioning

ROIABLE has an established presence in the SAP security ecosystem. The company was known mostly for its association with SAP IdM. Its work on SAP Business Technology Platform (BTP) has expanded its role in SAP cloud security. The introduction of ROI iAM shows strong knowledge of SAP on-premise identity solutions. It also shows the ability to use SAP BTP services for orchestration and continuity.

ROI iAM is a fully cloud based product. It does not use a subscription model. It offers the usual cloud benefits such as elasticity, scalability and AI capabilities. It avoids extra license cost and data transfer. This is achieved using a hybrid cloud deployment model where the solution runs in the customer's own SAP BTP subaccount. This removes the need to move security data between cloud providers. It also allows the customer to reuse existing SAP BTP purchased services.

ROI iAM supports the idea of a clean core in a security context. Many general purpose IGA tools offer standardized connectors and use cases. This works well for common scenarios; however, it is not always enough for complex and customized environments. ROIABLE suggests ROI iAM can adapt to specific security needs. It does this without requiring the leading IGA platform to handle every possible use case.

Architecture on SAP BTP

ROIABLE's architecture sits on SAP BTP and uses SAP Integration Suite for connectivity to SAP and non-SAP systems. The SAP Event Mesh capability enables asynchronous patterns for provisioning and callbacks. SCIM is used to expose the sidecar data model to the leading IAM. This approach separates the enterprise's IAM decision from downstream technical specifics where any leading IAM that speaks SCIM and can utilize the event-based communication that can drive the same provisioning and governance flows. Finally SAP Joule AI wraps all the information into an end-user experience for self-service. This offers the necessary bridge between the leading IAM platform and ROI iAM in the cloud. It acts

both as a translator and an orchestrator for what the end-user wants to request or validate with regards to their current or future access.

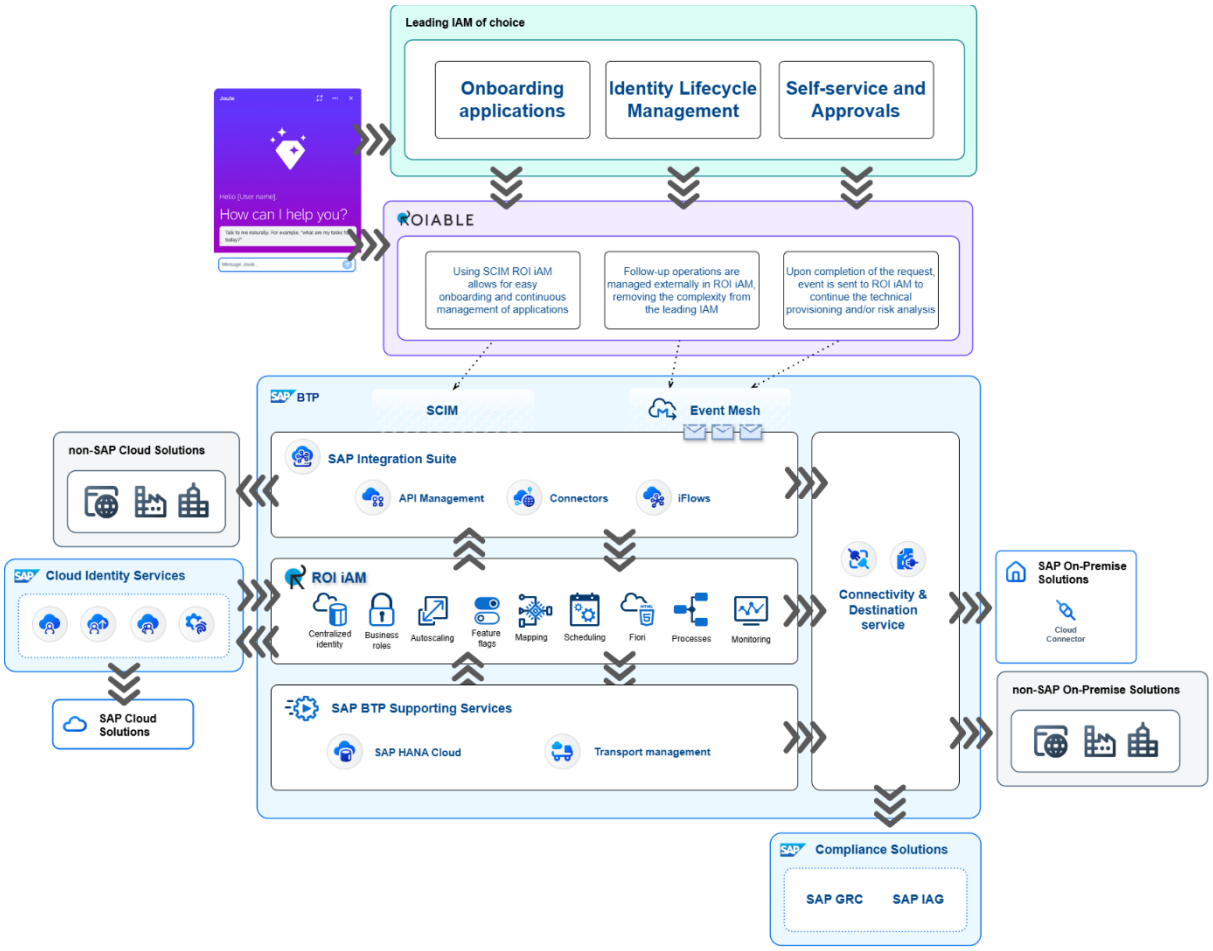

Figure 1: ROI iAM architecture (Source: ROIABLE)

Phased migration plan

ROIABLE migration methodology includes detailed step by step plan which is outlined as:

- Phase 0: SAP IdM Migration Analyzer by ROIABLE
- Phase 1: Connect sources to ROI iAM
- Phase 2: Step-wise migration of target connectors
- Phase 3: Optional: move SAP GRC connectors
- Phase 4: Redesign/move IAM lifecycle and approval processes to the leading IAM system
- Phase 5: Disconnect SAP IdM

Each phase comes with its specifics, which are discussed in a planning workshop together with ROIABLE, before each migration project start.

ROI iAM SAP IdM Migration Analyzer by ROIABLE

The Analyzer is setup on SAP IdM 8.0 (NetWeaver 7.5) and compares current packages against originals to classify objects as original, modified, new, or custom. It provides report jobs (users, attributes, entry types, forms without ACLs, processes used/unused, systems per repository) and estimation jobs that quantify modified scripts, used processes, and more. Results can be exported to CSV and analyzed in Excel. This creates an objective baseline and a defensible effort estimate for the migration program. What distinguishes ROIABLE in this field is the tool's ability to auto-calculate the estimated efforts required for migration. This is a feature that significantly reduces guesswork and provides precise estimates, saving time and resources.

The Analyzer's auto-calculation of migration effort is valuable but should be treated as a direction rather than a binding contract. Actual efforts depend on factors the tool cannot measure such as quality of documentation, availability of original developers, and business willingness to retire legacy workflows.

Organizations should validate estimates against manual sampling of 10-15% of custom objects before committing to project budgets.

Utilizing the SAP Integration Suite, ROIABLE offers over 400 connectors. Whether the data interaction involves REST, file-based databases, or other protocols, the SAP Integration Suite supports any system connection. Additionally, ROIABLE enhances connectivity with an event mesh, which not only provides flexibility but also supports the event-based interactions vital for modern IAM operations

SAP GRC risk analysis and provisioning accelerator

ROIABLE enables SAP GRC Access Control to act as a central risk analysis solution for systems across the customer landscape, including non-SAP systems. The accelerator positions SAP GRC for both provisioning-time checks and authorization analysis, converting target authorization structures into objects GRC understands. Integration uses SAP-standard connectors and is designed to minimize changes to existing SAP GRC logic and configurations. In practice, this lets organizations keep SAP GRC approvals and SoD analysis in place while replacing SAP IdM under the hood

The GRC proxy pattern preserves existing Access Control investments but also perpetuates dependency on SAP GRC, a product line that continues to be supported on SAP HANA, and its availability aligns with the broader SAP HANA support timeline Organizations should consider:

- Whether GRC licenses will remain available for purchase through 2040+
- If cross-system risk analysis could be achieved in the target IAM platform

Reporting dashboard

ROIABLE's reporting add-on provides modern dashboards with wide range of filtering options. It is currently available only for SAP IdM on-premises. ROIBALE suggests this reporting dashboard can be used for scanning through historical data once the migration has completed. This is essentially a crucial feature for audit and compliance purposes.

It decouples report access from SAP IdM roles, supports any device, and enables export for further analysis. During migration, the cockpit becomes the operational window into identity and access health for process owners and auditors.

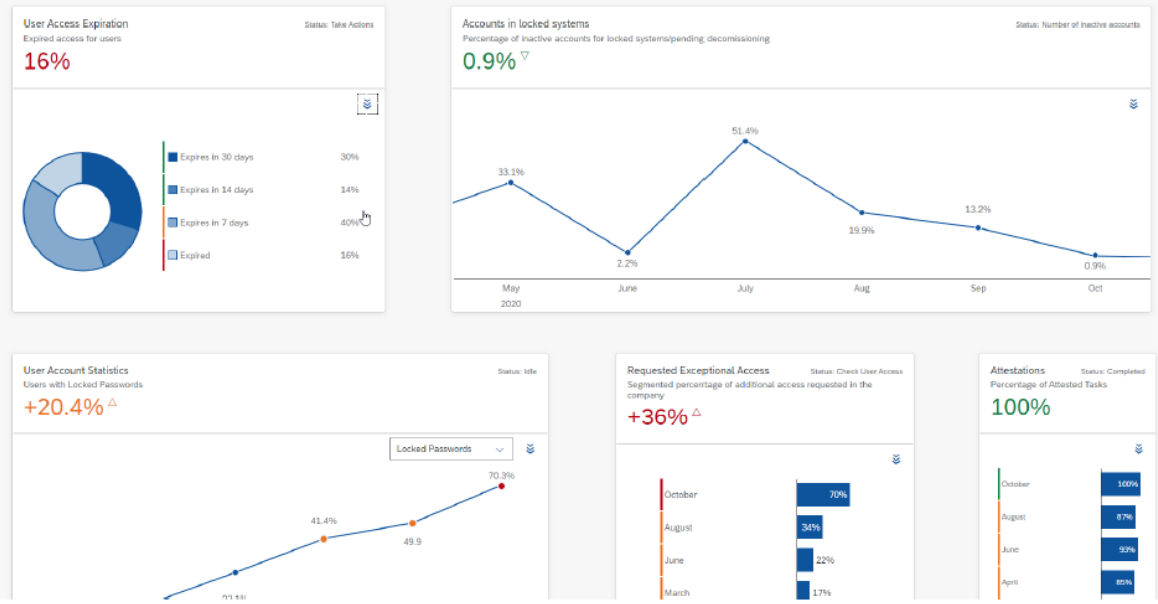

Figure 2: ROIABLE Reporting Dashboard (Source: ROIABLE)

The reporting features have multiple use cases which are as follows:

- **Available to authorized personnel:** This highlights that report access is separated from the roles and permissions within SAP IdM. Reports and dashboards are created using technical users, while an additional security layer ensures that only authorized viewers can access the data. This approach improves data security and simplifies access management.
- **Customizable per viewer:** This explains that each viewer can personalize reports according to their preferences. Users can define which columns to display, rearrange table headers, and save report templates for regular use. This customization empowers users to focus on the information most relevant to their roles and responsibilities.
- **Calculated dashboards:** Dashboards visualize complex IdM data, making it easier to interpret and drill down into details.

- **Data Filtering:** Additionally, users can filter SAP IdM information based on various attributes, including master and assignment data, and view or export results for further analysis in Excel.

SAP GRC risk analysis and provisioning accelerator

For the authorization scenario, ROI iAM refers to the target system's authorization structure and converts it to the standard objects recognized by SAP GRC. It stays available for SAP GRC's live calls during access requests and risk analysis. When a system is onboarded to SAP GRC via ROI iAM, provisioning completes by sending events and waiting for responses—keeping GRC the primary approval and policy layer while ROI iAM executes the technical changes.

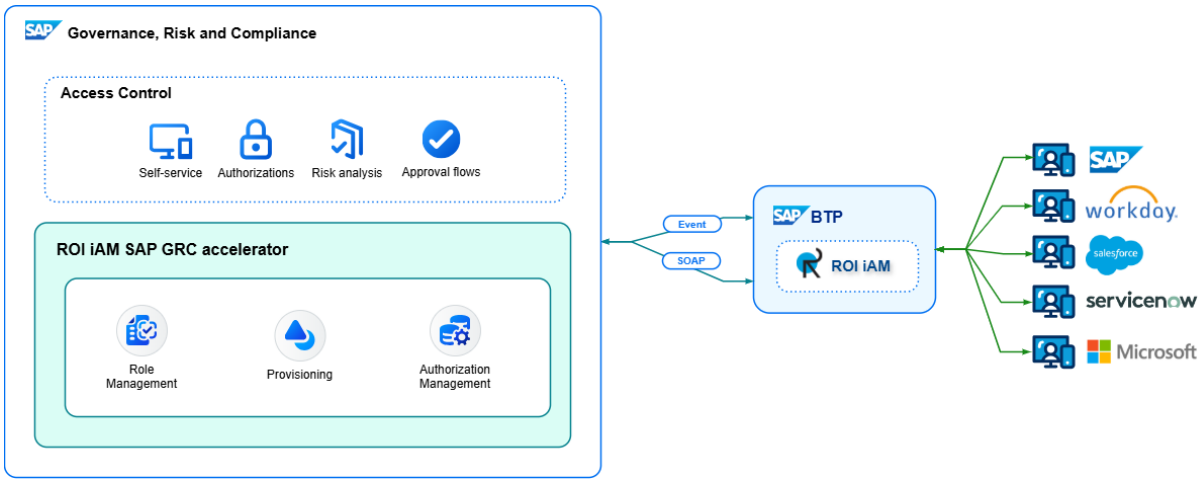

Figure 3: ROI iAM Integration with SAP GRC

Provisioning accelerator for Microsoft Entra

ROIABLE delivers applications that add event-based orchestration to Microsoft Entra. The accelerator supports workflows, Graph integration, app roles, and callback processing to and from ROI iAM. This enables MS Entra to become the leading IAM for SAP and non-SAP landscapes, especially if their security APIs are non-standardized (e.g. custom REST, File-based) or require custom logic to derive the proper roles/groups for the leading IGA. In the solution diagrams below, SuccessFactors is feeding the master data for the identities to Entra, which on its behalf is responsible for the self-service and approvals. Once those are through, ROI iAM performs the provisioning and makes a call back to Entra asynchronously.

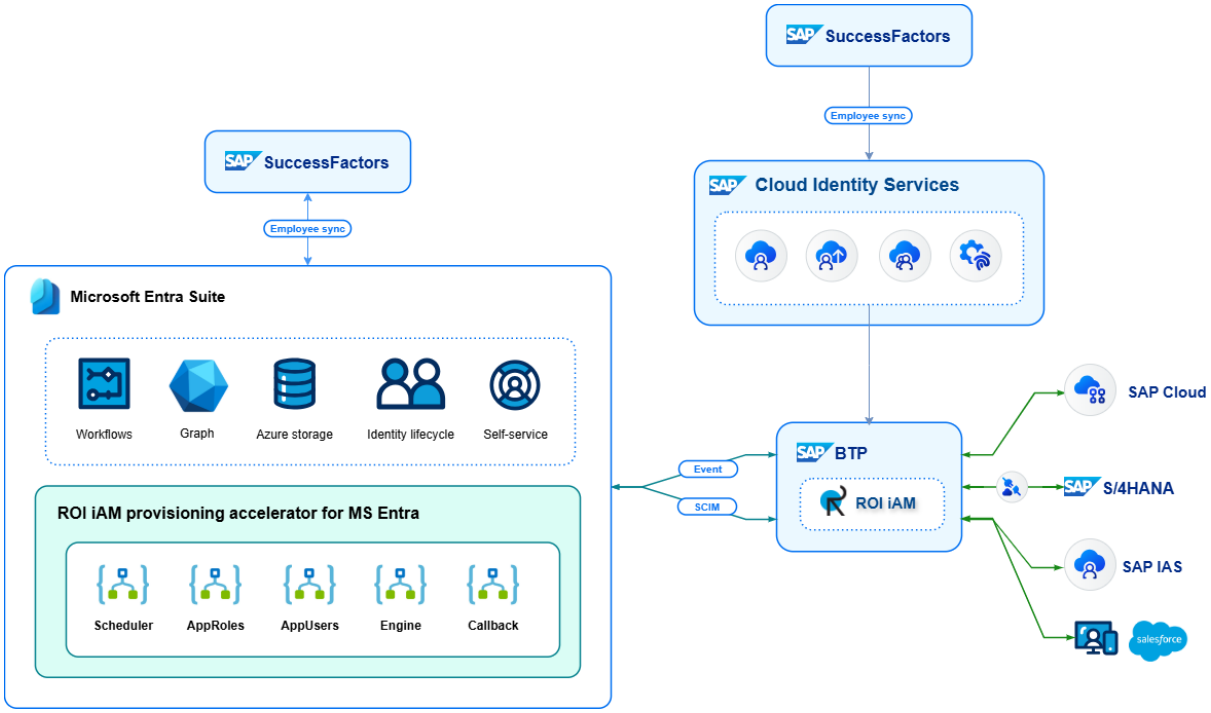

Figure 4: ROI iAM Microsoft Entra Connector

Impact on SAP GRC and SoD

ROIABLE's material outlines how SAP GRC Access Control remains the system of record for SoD and policy enforcement during migration, with ROI iAM acting as both a target and a proxy. This allows organizations to keep their established GRC processes while enabling cross-risk analysis between SAP and non-SAP systems—an important requirement for regulated industries

Operations and Change Management

ROIABLE delivers updates once every four months and aligning with enterprise expectations for predictable release trains. The event-driven model limits changes in the leading IAM and concentrates SAP-specific complexity within ROI iAM on SAP BTP—a division of responsibilities that many SAP customers prefer for maintainability

ROIABLE's event-based integration approach distinguishes their solutions in the market. This method supports a wide range of connectors, enabling organizations to adapt their IAM structures without overhauling existing frameworks. The general model does not require the integrated system to adjust to ROIABLE's data model. Instead ROI iAM adapts to the system being integrated. ROIABLE's focus on interoperability and scalability ensures a forward-compatible transition to modern identity solutions, minimizing disruption and maximizing efficiency.

Identity Lifecycle Management

ROIABLE's framework is not limited to integration and connectivity. The solution allows for advanced identity lifecycle management, handling application onboarding, user provisioning,

and access reviews efficiently. By adopting ROIABLE's identity lifecycle management strategies, organizations can ensure that user identities are managed in alignment with business policies while adhering to compliance requirements, thus mitigating risks associated with unauthorized access.

ROIABLE's system is designed for standardized onboarding processes that provide clear role definitions, policy alignment, and access control adjustments. These features are all automated to reduce administrative overhead. This structured approach also assists in minimizing human error and ensuring consistency in identity governance across the organization.

Within the domain of provisioning technologies, ROIABLE's solutions are geared to refine and enhance identity lifecycle management, application onboarding, and comprehensive user management. Their deployment model emphasizes minimal impact on user experience during the migration process, focusing on integral administrative functions to support continuous operation.

Conclusion

ROIABLE's contributions to IAM, particularly concerning SAP IdM migration, underlines its capability to deliver transformative solutions tailored to enterprise needs. As businesses prepare for the 2030 phase-out, ROIABLE's expertise in adaptive, future-proof identity systems provides a strategic edge. Their focus on integration, identity lifecycle management, and phased migration equips enterprises to transition smoothly and maintain competitive operations.

In summary, ROIABLE remains a defense against the uncertainties of a complex system migration. By embedding flexibility, automation, and strategic foresight into its products, ROIABLE ensures that organizations are not only prepared for today's identity management challenges but are also poised to navigate the evolving landscape of tomorrow with confidence.

Recommendations

Effective SAP IdM migration requires translating insight into structured action. The following recommendations summarize the essential steps organizations can take to maintain governance, ensure operational continuity, and achieve a controlled transition before SAP IdM reaches its end of life.

For Organizations Planning SAP IdM Migration:

- **Begin with discovery, not selection**: Use an analyzer tool or manual audit to quantify migration scope before evaluating target platforms. Organizations that select replacement IAM first often discover mid-project that critical SAP IdM capabilities have no equivalent.

- **Preserve GRC investment if already deployed**: SAP Access Control remains viable way beyond 2030. The effort to rebuild SoD rules in a new platform typically exceeds the cost of proxy integration patterns.
- **Plan for parallel operation of 12-18 months**: Sidecar architectures introduce operational overhead but reduce cutover risk. Budget for duplicate licensing and extended team capacity. However, this is compensated by reduced future investment in SAP IdM.
- **Establish objective completion criteria before starting**: Define measurable thresholds for provisioning accuracy, certification completion rates, and audit trail equivalence. Without these, migration programs extend indefinitely.
- **Inventory before migrating**: Prioritize used, business-critical objects. Organizations that attempt full object migration ("lift and shift") waste 30-40% of project budget on obsolete configurations.
- Determine whether the organization will renew SAP GRC Access Control licenses through 2030. If not, plan the migration or upgrade path to SAP GRC or HANA from 2026 so that GRC modernization can run in parallel with IdM migration

For Vendors and Service Providers:

- **Offer fixed-price discovery phases**: The most significant migration risk is scope uncertainty. Structured analysis services with capped fees reduce buyer hesitation.

Related Research

Buyer's Compass: Data Security Platforms
Leadership Compass: Policy Based Access Management
Leadership Compass: Data Leakage Prevention
Leadership Compass: Data Governance
Leadership Compass: Access Control Tools for SAP environments

Copyright

KuppingerCole Analysts supports IT professionals with exceptional expertise to define IT strategies and make relevant decisions. As a leading analyst firm, KuppingerCole offers firsthand, vendor-neutral information. Our services enable you to make decisions 1 to your business with confidence and security.

Founded in 2004, KuppingerCole is a global, independent analyst organization headquartered in Europe. We specialize in providing vendor-neutral advice, expertise, thought leadership, and practical relevance in Cybersecurity, Digital Identity & IAM (Identity and Access Management), Cloud Risk and Security, and Artificial Intelligence, as well as technologies enabling Digital Transformation. We assist companies, corporate users, integrators, and software manufacturers to address both tactical and strategic challenges by making better decisions for their business success. Balancing immediate implementation with long-term viability is central to our philosophy.

For further information, please contact clients@kuppingercole.com..