

Application Access Governance for SAP

Reducing Fraud, Compliance Risk, and Identity-Driven Security Risk Across Enterprise Applications



Enterprise Risk Lives Inside Your Applications and Infrastructure

SAP systems sit at the center of many of your most critical financial control and operational processes. Vendor payments, journal entries, procurement approvals, financial postings, and sensitive data access all depend on properly governed access across ECC, S/4HANA, hybrid landscapes, and the broader enterprise application ecosystem.

Access within SAP is governed through roles, authorization objects, transaction codes (t-codes), and Fiori applications. This results in a highly granular entitlement model that is difficult to govern at scale.

When access inside these systems is excessive, conflicting, or poorly monitored, the impact is immediate and material. Risks include:



Fraud exposure through toxic combinations of access



Regulatory violations and audit findings



Identity-driven security breaches from compromised credentials



Persistent privileged access that undermines Zero Trust



Escalating operational and license costs

Traditional SAP governance approaches were designed for static, single-application ERP environments and break down in today's complex, interconnected enterprise landscape.

Without unified visibility across SAP and connected enterprise systems, risk relationships remain hidden and violations are often discovered only after financial, compliance, or security damage has occurred.

Why Traditional Governance Breaks Down

Traditional SAP governance approaches were designed for static, single-ERP environments. Today's enterprise landscape surrounding SAP has become far more complex:

- Integrated across multiple ERP and business platforms
- Connected to SaaS applications such as Salesforce, ServiceNow, and Workday
- Operating across hybrid and multi-cloud infrastructure (AWS, Azure, GCP)
- Managing rapidly expanding identity populations, including employees, contractors, non-human identities (NHIs) such as service accounts and bots, and emerging AI agents and autonomous identities

As a result, traditional governance tools struggle to correlate cross-application Separation of Duties risks, detect identity-driven exposure across interconnected systems, or enforce continuous controls across SAP, enterprise applications, and infrastructure.

Periodic access certifications further compound the problem. These point-in-time reviews often lack visibility into underlying SAP privileges and real-world usage, including role assignments, authorization objects, and transaction code (t-code) activity, leaving reviewers without the context needed to identify and prevent risk before it materializes.

The Cost of Unmanaged Access



of employees have excessive application access to data. Excess access inside business systems creates hidden fraud, compliance, and security exposure.



of breaches involve stolen or compromised credentials² Identity misuse remains the primary attack vector.



of annual revenue is lost to fraud each year³ Access misuse directly impacts financial performance.



average cost of compliance violations for large enterprises⁴ Weak access controls drive measurable regulatory and financial exposure.

Sources: [Ponemon, Verizon Data Breach Investigations Report](#), [ACFE Report to the Nations](#), Industry compliance research.

A Modern Approach to SAP Application Access Governance

Reducing fraud, compliance, and identity-driven security risk across SAP and connected enterprise systems requires converged identity security applied directly within enterprise applications.

Saviynt Application Access Governance provides:

- Unified governance across SAP, SaaS platforms, cloud infrastructure, and enterprise applications
- Cross-application and cross-ecosystem Separation of Duties intelligence including SAP transaction codes (t-codes), authorization objects, Fiori objects, oData services, and application roles
- Continuous compliance and audit-ready controls across SAP and connected business systems
- Zero Standing Privilege enforcement with Just-in-Time access for SAP ERP and SaaS applications
- AI-driven risk detection, prioritization, remediation, and access reviews

Delivered as a single cloud-native AAG solution for your application ecosystem, combining governance, privileged access controls, and identity posture intelligence without stitching together fragmented SAP governance, identity, and privileged access tools.

Enterprise-Grade Security & Regulatory Trust



FedRAMP Moderate Authorized | SAP Certified | SOC 2 Type II | ISO 27001 | PCI-DSS | DORA-ready

Why Saviynt AAG Is Different

Converged Identity Security Platform

Saviynt AAG includes the governance, privileged access controls, and identity posture intelligence capabilities traditionally delivered by separate IGA, PAM, and ISPM tools within a single converged solution across SAP and the broader enterprise application ecosystem.

Govern all identity types

Enforce consistent controls for workforce users, contractors, non-human identities (NHIs) including service accounts and API keys, bots, and emerging AI agents, closing governance gaps many legacy SAP governance tools were never designed to address.

True Cross-Application & Cross-Ecosystem Intelligence

Correlates risk across SAP, SaaS platforms, cloud infrastructure, vendor ecosystems and custom applications, which expose toxic access combinations that traditional SAP governance tools cannot detect. This enables continuous control monitoring and more effective risk management.

Deep, Application-Native Entitlement Models

Understands SAP transaction codes (t-codes), authorization objects, role hierarchies, and organizational-level restrictions along with cloud IAM permissions and granular application roles rather than just user accounts.

AI Embedded Across the Identity Lifecycle

Applies AI-driven risk scoring, prioritization, automated remediation, onboarding acceleration, and certification optimization to reduce noise and accelerate time-to-value.

Zero Standing Privilege at the Application Layer

Enforces Just-in-Time and emergency access controls directly within SAP and other critical business systems aligning with Zero Trust principles while maintaining business continuity.

Single Platform. Lower Operational Overhead.

Consolidates fragmented SAP governance, identity, and privileged access tools with one converged platform that reduces audit scope, release testing effort, training complexity, and total cost of ownership.

Measurable Business Outcomes

Organizations achieve enterprise-wide impact across risk reduction, compliance, and operational efficiency across SAP and enterprise applications:



Up to **70%** reduction in Separation of Duties (SoD) violations



Up to **60%** lower identity administration costs



60% fewer false-positive risk alerts for faster threat response



15-25% reduction in ERP license costs



Access provisioning reduced from days to hours



Core applications onboarded in days, not weeks



30 days from purchase to value

Next Step

- Schedule a personalized executive briefing
- Request a rapid AAG risk assessment
- Explore a 30-day proof of value

About Saviynt

Saviynt's AI-powered identity platform manages and governs human and non-human access to all of an organization's applications, data, and business processes. Customers trust Saviynt to safeguard their digital assets, drive operational efficiency, and reduce compliance costs. Built for the AI age, Saviynt is helping organizations safely accelerate their deployment and usage of AI today. Saviynt is recognized as the leader in identity security, with solutions that protect and empower the world's leading brands, Fortune 500 companies, and government institutions. For more information, please visit www.saviynt.com.



Headquarters
1301 E El Segundo Blvd,
Suite D El Segundo, CA 90245
United States

310.641.1664
info@saviynt.com
www.saviynt.com