EBOOK

Securing Application Access During ERP Modernization

EY Building a better working world

Saviynt

Contents

Introduction

Digital transformation is reshaping how businesses operate, introducing new ways to stay competitive and innovate. Modernized IT infrastructure is central to this, including Enterprise Resource Planning (ERP) system upgrades.

While reasons to upgrade ERPs vary, end-of-maintenance announcements from traditional vendors will fast track organizations into the process. For instance, SAP has announced that standard maintenance for its popular on-premises ERP system (ECC 6.0) will be ending. Oracle and Microsoft made similar pronouncements — and each affect the identity; governance, risk, and compliance (GRC); and security tools that enterprises rely on.

Transitioning ERPs brings opportunities to strengthen security, stay compliant with evolving regulations, and safely integrate new platforms with existing applications.

In this eBook, we explore how a modern identity access governance platform – deployed alongside a new ERP – helps organizations monitor, analyze and manage access risks in real-time. We also highlight strategies for managing access, risk, and compliance and explore how an advisory and technology service partner can facilitate readiness and integrate risk management and compliance into the process.

What's at stake: Application risk in ERP transformation

As businesses move sensitive finance, accounting, and payroll data to modern ERP applications, ensuring compliance grows more critical – and complex. Presently, up to **one-third of all** application hacks result from unauthorized access via default, shared or stolen credentials.

A Saviynt and Ponemon Institute State of Enterprise Identity survey of 1,000 IT and security practitioners **found that** 46% of organizations failed to comply with regulations due to access related issues.

Each ERP and critical business app that an enterprise relies on correlates to hundreds of functions, potentially to thousands of people. And one wrong role with the wrong type of access creates toxic combinations. Regulations like Sarbanes Oxley (SOX) or the Graham-Leach-Bliley Act (GLBA) impose stiff penalties for separation of duties (SoD) violations.

What exacerbates application access risk?

Historically, companies targeted single ERP systems, enticed by the potential of "one system to rule them all." The appeal made sense – a unified system that could eliminate data silos, standardize processes, streamline management and deliver a single source of truth.

But enterprises ran into issues with large, inflexible systems and found benefits by adopting best-of-breed solutions for specific functions (e.g., Workday for HR, Salesforce for CRM, and NetSuite for financials.) SaaS tools excel for specific use cases in ways that the "jack-of-all-trades" ERP systems couldn’t.

As such, few organizations rely on a single vendor to provide their enterprise applications. Cloud-based, best-of-breed applications now supplant (or complement) traditional solutions. This dynamic results in unique governance challenges.

Using SAP as an example, the transition away from on-premises ECC and SAP S/4HANA®, as well as the end of maintenance for SAP IDM, presents an opportunity to modernize security strategies, adapt to a dynamic environment, and explore innovative solutions for identity and governance management.

Enterprises now need to **reevaluate identity and access management** needs, examine the deficiencies of replacement “point” solutions, and consider identity-centric security approaches that work with their varied apps and identity types. They will also need to account for how these work across on-premises, cloud, and hybrid ecosystems.

Although legacy providers may promote new tools for identity governance and app GRC, poor cross-application performance and issues related to an on-prem to cloud transition may persist. For those considering point solutions, Vinit Shah, Vice President, Product, Saviynt highlights the limitations of more traditional access governance tools.

“Identity governance offerings from legacy ERP providers have limited integration capabilities with other systems and applications. This makes it difficult to streamline control processes, share data, and achieve a holistic view of governance, risk, and compliance activities,” suggests Shah.

Begin transformation with the end in mind

ERP transformations expose and exacerbate underlying risks surrounding GRC. Concerningly, modernization project plans often underestimate the necessity of developing appropriate control structures to mitigate SoD issues and other pressing risks.

The ERP platform is not the only software undergoing transformation. One cannot lose sight of compliance requirements across the interconnected ecosystem of applications when upgrading or transitioning ERP systems.

According to Natalie Freedline, Principal, Technology Consulting, at Ernst & Young LLP, organizations tend to overestimate security preparedness in their modernization campaigns.

“Any ERP transformation or upgrade is inherently risky, and organizations should not assume that their existing internal controls governance, business processes, and operating support models are flexible or robust enough to support the future state,” shares Freedline.

> **“Leading practice for GRC models is to create standardized, measured, controlled, repeatable processes that allow for continual improvement and optimization. Without proactive planning and purpose-built tools, you may miss out on some value adds to your business and major ROI.”**
>
> –Natalie Freedline, Principal, Technology Consulting, at Ernst & Young LLP

Project teams need to develop security roles to remain compliant and SoD conflict-free as transformation projects unfold.

Ideally, enterprises **capitalize on** the simplicity of a single project management framework, common methodology, and fully-aligned team to improve compliance capabilities in tandem with an ERP upgrade.

In discussing the benefits of proven methodologies and an audit-aligned approach to improving controls in an ERP upgrade, EY’s Freedline shares that proactive global solution design “is an essential part of risk reduction and makes it easier to embed compliant security and business or IT controls.”

Steven Oberhauser, Senior Director, AAG Solution Leader, notes that upstream work to improve a compliance program will “reduce manual efforts with controls automation and optimization, harmonize security design across multiple systems, and simply deliver more effective control performance.”

Application access governance in a modern world

As traditional ERPs are sunset away, CISOs must investigate replacing risk analysis and provisioning security tools. Security leaders will also plan towards redesigning access controls for the cloud-based ERP and interconnected applications.

In this, leaders face a fundamental question:
Do I move forward with multiple point solutions that address only certain capabilities that my existing identity governance and application GRC solutions delivered?

Or should I centralize as much as possible to help with management, productivity and costs?

ERP transitions often highlight opportunities to unify application security. At this crossroads, access governance can be strengthened, improving the ability to detect anomalous activities and address material deficiencies.

Often, ERP transitions heighten (or expose) poorly unified application security. And at this crossroad, access governance issues intensify, exposing challenges like spotting anomalous activities and propagating material deficiencies.

Along these lines, Oberhauser warns that the breadth of applications enterprises use heightens cross-system SoD risks. “Problematically, organizations may default to a point solution or cobble together third-party connectors. As a result, they lack fine-grained visibility of the application ecosystem and rely instead on rigid rules without context awareness.”

Although the days of using one vendor for critical applications have passed, some organizations try to stretch a single identity security tool across their varied ERP and business applications.

Relying on traditional vendors to deliver modern app GRC introduces challenges, including:

- **Reinforcing silos from a lack of cross-application support**
- **Increasing customization (read: complexity and cost) to support cross-application management**
- **Difficulty managing access at a fine-grained level for all applications**
- **Non-availability of continuous controls monitoring and emergency access management for applications**
- **Missing identity context and visibility for supplier, contractor, non-human and bot identities**
- **Inability to automate and/or manage Joiner, Mover, Leaver events**

As organizations adopt cloud-based solutions, business models and operations are transforming. For many, the volume of interconnected line-of-business applications is increasing. These changes introduce opportunities to enhance security strategies and effectively manage the different security models of non-SAP applications.

Digging deeper into ERP Migration Challenges

A common set of essential tasks emerges during migration from an on-premises solution to a cloud-based solution. In general, organizations must address some (or all) of the following.

Addressing prior customizations: Cloud platforms prioritize standardization, meaning, existing customizations may not translate to the new platform.

Organizations need to assess what can migrate, along with their capacity to redesign customizations. Some customizations, including code, integrations and workflows may be needed for regulatory compliance, especially for those in regulated industries.

Role re-design: Companies need to understand required role upgrades and authorizations. For example, there can be new checks for authorization objects and new transactions taking place post migration.

As well, design changes can impact users' understanding of how to build roles, adding difficulty for those not familiar with a new framework. In particular, challenges emerge around coordinating various access types, especially if the access needs span hybrid landscapes.

License management: Licensing models will differ between different deployments, and organizations need to ascertain how these affect total-cost-of-ownership (TCO).

Costs: Redevelopment work and licensing implications add unexpected expenses. In particular, redevelopment costs quickly add up for those with extensive modification or customization needs.

Companies need to combat these challenges, while also addressing follow-on questions surrounding their appetite to build connectors for new applications, investing in further role and privilege access design, or cleaning data. Each is essential for maximizing security and functionality, and minimizing downtime during migration.

Conquering challenges with modern tools

Modern application access governance solutions unwind the complexities of managing multiple GRC access control solutions and eliminate the gaps left by point solutions across applications including SAP, Workday, Active Directory, EPIC, and more.

Saviynt Application Access Governance (AAG) unifies ERP and line-of-business application security models under a single umbrella to standardize controls across any environment. When enterprises transition their ERP, designed integrations increase visibility and risk detection, allowing organizations to identify risks and anomalous activities more effectively.

> **“Growing use of diverse apps, coupled with end-of-maintenance for solutions like Oracle and SAP GRC, means companies must reevaluate their access governance strategies and consider more comprehensive and integrated identity security.”**
>
> –Vinit Shah, Vice President, Product, Saviynt

Traditional GRC or identity solutions underperform when assessing SoD violations across multiple, disparate applications. Beyond this, security administrators must pull dissimilar data from these apps and manually review outputs to identify issues. This is time consuming, costly, and inaccurate.

A modern solution aligns security policies across all applications, devices, and operating platforms. Across these, security leaders can use granular entitlement governance, detecting and preventing cross-application SoD violations before they occur.

For enterprises transitioning ERPs, upgraded GRC capabilities means SAP, Oracle, Microsoft, or other traditional shops can adopt one solution to support access governance for a range of platforms and critical applications and maintain audit readiness. The design eliminates silos and reduces implementation times, management costs, and administrator burnout.

Moreover, improved application access governance helps enforce least privilege policies and unlocks a core component of compliance: continuous controls monitoring (CCM).

CCM brings new levels of intelligence to access security and helps establish analytical controls mapped to compliance regulations, like PCI, SOX, GDPR, ISO, and others. Saviynt’s Oberhauser believes enterprises should move past periodic assessments, but warns that “few traditional solutions offer continuous control monitoring and real-time or near-real-time insights into control performance.”

Instead, organizations succumb to audit fatigue (or worse) and without CCM, struggle responding to new threats, vulnerabilities, or regulatory requirements.

With capable CCM, organizations **introduce** real-time data monitoring and continuous surveillance of IT systems. Beyond surveillance, CCM drives compliance management by collecting not just present-state data about controls, but also supports real-time updates, automated reporting, and resource optimization.

ERPs & GRC: How EY enables security excellence

The ERP transformation journey offers organizations an opportunity to reduce their risk posture and reduce compliance costs by streamlining business processes and IT controls.

But successful outcomes run on the tracks of 1) a proven methodology, and 2) an audit-aligned approach. Together, these help enterprises mitigate ERP transformation risks around application security and GRC enablement and controls.

Enterprises need to update their controls framework to reflect future state expectations. However, most implementations underestimate (or ignore) the need to develop appropriate control structure to mitigate risks.

“Process redesign”: core to ERP transformation.

EY’s Freedline believes that successful enterprises operate with a key distinctive: “They fight the temptation to leave control issues until the end of the ERP transition.”

For this, internal controls stakeholders must be engaged in scoping and evaluating processes early-on. This is important because most enterprises face a common set of governance risks when modernizing ERPs, often including –

- Inefficient, overly manual business process controls
- Imbalanced application security impacting user access management and compliance
- Controls and security weaknesses that are not discovered prior to going-live
- Highly localized and differentiated access controls based on capabilities of legacy applications
- Increased compliance expenses, including increased/ unmanageable SOD and sensitive access risks.

The above issues result due to poor preparation, and organizations should avoid ERP transitions without an accompanying security strategy. Alongside, they should not forgo a current state risk assessment, or deploy ERP software without a robust controls design or plan.

Freedline warns: “When organizations operate without a global, organized process for security and controls, they find themselves later constrained — lacking agility and ‘recreating the wheel’ when designing proper access controls across new applications and environments.”

They then deal with increased compliance expenses and unmanageable SoD and sensitive access risks — often ones that were avoidable.

Prepared organizations comprehensively plan and reduce risk by embedding compliant and extensible security and business/IT controls by design. The genuine collaboration pays off: enterprises reduce the time and resource investment required to gather, assess, and detect control weaknesses or inadequacies.

“This unlocks the capacity for security leaders to remediate deficiencies and prevent recurrence from repeating in the future,” shares Freedline.

An experienced services provider intuits resource and planning constraints alongside compliance demands. With this insight, it can help organizations write a roadmap for building application rulesets and identifying user access risks to be remediated.

Although an oversimplification, consider the following illustrative planning stages and ask: To what extent is my organization able to embed these elements into a transformation initiative?

Foundation

- Perform detailed risk and controls assessment of newly designed business processes
- Design/build and test controls and align with internal and external audit requirements
- Understand security requirements to develop a global template with a modular and scalable role design
- Define SoD sensitive access risks as part of the global template framework and as appropriate for a pilot
- Deploy access governance to support global implementation program
- Facilitate the application of roles to users and provision appropriate access
- Design roadmap and strategy to use controls automation

Frame

- Extend global template role design based on additional markets or LOB requirements
- Establish POC for GRC process and enabling continuous controls
- Assess ERP for security vulnerabilities and misconfigurations
- Design, build and deploy controls for local customizations and/or rulesets not provided out-of-the-box

Finish

- Sustain controls monitoring and alignment with auditors
- Maintain business process and controls governance
- Support enterprise risk management and better governance through global standardization

No one right way for process redesign exists. However, a tried-and-true process surfaces real-time visibility of potential risks before issues become material. Most important, however, is that enterprises resist the tendency to treat security as an afterthought in ERP transformation.

According to Freedline, the benefits of improving controls in parallel to ERP transitions outweigh the effort: “With the right strategy and proactive risk management, organizations can handle the challenges of securing systems, integrating multiple softwares, and managing user identities and access privileges across any new applications.”

Saviynt & EY: Better Together

For enterprises modernizing ERPs, the EY and Saviynt alliance supports simpler access governance and helps organizations manage security and compliance risks for their on-premises, cloud, and hybrid business applications. The comprehensive partnership involves redesigning access control models for modern ERPs (SAP, Oracle, Workday, etc.), and building well-optimized identity security programs that account for enterprise and line of business applications.

With extensive implementation experience of Saviynt AAG and the **Identity Cloud,** EY is positioned to guide integration and help organizations optimize access management and controls as they reinforce GRC capabilities, and reduce governance costs related to manual processes and limited intelligence.

If you’re evaluating a move to SAP S/4HANA or another cloud solution but are concerned with maintaining security throughout the process, **reach out to Saviynt** to discover how The Identity Cloud supports SAP and other ERP ecosystems. As well, connect with EY to learn about advisory services surrounding migration.

Saviynt

Saviynt empowers enterprises to secure their digital transformation, safeguard critical assets, and meet regulatory compliance. With a vision to provide a secure and compliant future for all enterprises, Saviynt is recognized as an industry leader in identity security whose cutting-edge solutions protect the world's leading brands, Fortune 500 companies and government organizations. For more information, please visit www.saviynt.com.

EY Building a better working world

EY is building a better working world by creating new value for clients, people, society and the planet, while building trust in capital markets.

Enabled by data, AI and advanced technology, EY teams help clients shape the future with confidence and develop answers for the most pressing issues of today and tomorrow.

EY teams work across a full spectrum of services in assurance, consulting, tax, strategy and transactions. Fueled by sector insights, a globally connected, multi-disciplinary network and diverse ecosystem partners, EY teams can provide services in more than 150 countries and territories. All in to shape the future with confidence.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

Saviynt

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

310. 641. 1664 | info@saviynt.com
www.saviynt.com