SailPoint

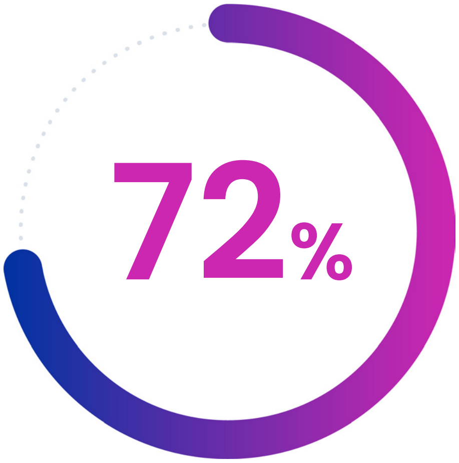
eBook

Five tenets of holistic access governance for SAP

The explosion of technology and cloud applications has simplified the way we work. But at the same time, the business systems that contribute to digital transformation and drive greater efficiencies have complicated security.

According to a Zylo Inc. report, the average enterprise **has about 600 SaaS applications** in use. The greatest threat involves access to key systems, such as SAP, that run critical processes, contain sensitive data, and have complex levels of access control. Those access risks may stem from external sources or internal authorized users.

The lack of uniform controls across a multitude of applications compounds the problem. Some systems may be without controls while others may be managed with manual processes. It's also possible that there are different control solutions in use across varied applications. Such disparity can lead to inconsistent, non-conforming access, time-intensive and error-prone monitoring, increased threats, fraud, and audit deficiencies.



Increase in actionable insider threats in 2021[1]

[1] DTEX 2022 Insider Threat Report

A **recent and large case of corporate fraud** proves how devastating fraud, caused by a lack of uniform controls, can be and how long it can go undetected. In April 2021, the former chief financial officer of the Alden Shoe Company pled guilty to embezzling approximately $30 million from the organization as part of a long-running scheme. This included writing checks to himself from company bank accounts and transferring funds from company accounts to his personal accounts and to another individual.

SAP and other enterprise resource planning (ERP) systems are particularly challenging because they process a company's most sensitive data and financial transactions. According to SAP's January 2021 corporate fact sheet, **77% of the world's transaction revenue** is handled by an SAP system. Complicating access governance further is the myriad of other cloud applications used alongside SAP ECC. This is even more complex with S/4HANA and the introduction of the cloud application ecosystem, where applications such as SAP SuccessFactors (for human capital management) reside outside of the S/4HANA business core. In a network of separate applications, real-time, intelligent understanding of access – and all the potential risks – is critical for protection against fraud, data theft, and employee mishaps.

If the outlook for SAP business transformation is through expanding adoption via cloud applications, how should businesses be thinking about access management in order to maintain controls and reduce risks in such a dense network? The following are the five top tenets smart companies are embracing.

1. Technology should govern technology

Today, manual access controls pose a serious risk because human-based approaches simply can't scale with the speed, visibility, and accuracy needed to identify risks in one ERP, let alone multiple systems. To put this in context, in the time that it takes to generate access reports and review them in accordance with access rules, roles and policies, new risks could emerge and, therefore, be missed. Automated, real-time, and continuous analysis is necessary to fully protect against risks, something that's impossible with a manual approach.

Go deep with Granular Utilization Insights

Additionally, full disclosure of risks requires analyzing not just users but also roles and business processes. Dictating what a user can do in a system is one thing but being able to see a user's actual usage is another — and this is crucial in order to have full visibility. A complete spectrum of risk identification is impossible without technology that can automate analysis on an ongoing basis at a deep and granular level of utilization.

Manually provisioning access or granting emergency access for elevated or short-term use has similar risk ramifications. The additional effort involved is challenging enough, but the danger of granting access without understanding potential risks ahead of provisioning is particularly precarious. Ideally, a company should have the ability to simulate risks that could occur so that new risks aren't introduced into the system. This is an essential instant safeguard only possible through automation. Predictive risk analysis makes it possible for companies to:

- Analyze risk before provisioning to prevent new risks
- Predict the impact of changes on any given role
- Elevate access or grant emergency access without risks

Also, with manual emergency provisioning, there is a significant chance that access won't be revoked at the access expiration date. The result: yet another threat to the system.

All of this said, technology alone is not enough. Automated access control solutions for SAP should help you achieve several other objectives, such as unifying controls and risk data to meet the demands of environments with extensive applications in use.

2. Centralize Insights

Controls for a mix of applications also need to work together to deliver the most accurate and efficient access management and risk insights. Without the same access controls across applications, companies can't immediately see the whole range of risks for users, nor can they conduct holistic analysis, reporting, and reviews. Disparate systems cause fragmented risk information that is harder to turn into actionable data intelligence. Time is critical in spotting and stopping risks. The longer a threat persists, the more costly and damaging it is.

For example, an insider incident recovered in less than 30 days has an average **annualized cost of $7.1 million** while an incident that takes more than 90 days to remediate will cost $13.7 million. If a user has violated permissions and committed system offenses in one application, the ability to see if similar activity has occurred across other systems is essential in stopping threat actors and insider incidents alike.

3. Integrate identity security and SoD access controls

Comprehensive and all-inclusive access controls are a powerful advantage, yet even bigger gains can be achieved when both SoD monitoring and identity security are merged into a single solution.

Unified identity security with granular access controls provides a double layer of security: It protects the perimeter while securing the interior. There is the assurance that only credentialed users with added authentication checks are getting into a system, along with visibility into what those users are doing once inside. When this happens across multiple applications, continuously, companies benefit from true enterprise-wide risk knowledge and security. It's 360° protection.

4. Reduce audit and compliance complexity

Replacing flawed manual processes with automated ones can also eliminate excessive audit work, improve the completeness and accuracy of audits, and help companies stay fully compliant. A reduction of risks and a decrease in material weaknesses are more likely, along with a reduction in audit costs, fines, and fees. Boards, investors, and customers will have more confidence in companies that breeze through audits without fail.

Periodic access reviews are an important part of audit and compliance. Done right, a company can cut audit and compliance complexity. Done wrong, risks remain undetected, audit deficiencies can occur, and costs can soar. And reviews should not be just an annual task. For the greatest risk prevention, reviews should be done more frequently, which is challenging if not impossible without automated SoD monitoring, reporting, and reviews across all applications.

5. Think holistically

True transformation and complete identity security require a company-wide strategy that puts equal emphasis on preventing both internal and external threats, as well as ending siloed risk management. Company stakeholders need to be on the same page with this approach.

True transformation requires a company-wide strategy

Any division in thinking about the importance of broad and deep protection – and how to achieve it – needs to be addressed through education and by involvement of more than IT and security teams. Audit, compliance, finance, and C-level employees also need to be involved for buy-in.

Additionally, teams need to think holistically when it comes to implementing new applications. Implementation projects need to go beyond merely deploying a system and should include taking combined identity and access controls into account from the start. The implementation of SAP S/4HANA is a good example. KPMG estimates that remediation work post-migration can cost as much as **30 times** more than if controls had been included in the initial requirements.

Conclusion

The use of technology to conduct business more efficiently will only increase – not just for SAP customers but for all businesses. And more of those technologies will be cloud applications; Gartner forecasts a **20.7% increase in cloud spending in 2023**. The use of cloud security solutions is also expected to increase, and that makes sense. The greatest flexibility and scalability are experienced with cloud tools. This is particularly true with SoD monitoring and identity governance.

Unifying access controls for multiple solutions with seamlessly integrated identity security brings risk management processes and visibility together in one platform for holistic, enterprise-wide access governance and protection. Using cloud access risk management solutions increases the benefits and can deliver faster time to value with fewer long-term expenses and challenges.

SailPoint®

About SailPoint

SailPoint is the leading provider of identity security for the modern enterprise. Enterprise security starts and ends with identities and their access, yet the ability to manage and secure identities today has moved well beyond human capacity. Using a foundation of artificial intelligence and machine learning, the SailPoint Identity Security Platform delivers the right level of access to the right identities and resources at the right time—matching the scale, velocity, and environmental needs of today's cloud-oriented enterprise. Our intelligent, autonomous, and integrated solutions put identity security at the core of digital business operations, enabling even the most complex organizations across the globe to build a security foundation capable of defending against today's most pressing threats.