APPSIAN

SAP Security Report:

Executive Perspective On SAP Business Risk Management

Critical ERP applications like SAP ERP Central Component (ECC) and S/4HANA support the foundation of business operations. In February of 2020, Appsian commissioned a third-party consulting agency to survey nearly 200 senior stakeholders at organizations using SAP ERP applications to uncover their top concerns in the governance, risk, and compliance space.

Introduction

The core of any organization is its data – whether business, financial, or HCM. This data represents the crown jewels. Given the critical nature of this data and increasing risks around it, organizations rightfully prioritize cybersecurity investments to protect their crown jewels. However, the task of securing ERP data differs vastly from the traditional IT security approach.

Today's rapidly changing landscape, coupled with the inherent complexities of SAP, has surfaced challenges in organizations trying to maintain a strong security posture while enabling productive business processes.

We found that this pace of change has brought about a new normal for accepted risk in SAP – but not by choice. While some organizations have adopted new processes and technology to address risk, legacy strategies are holding many back in their path towards efficiently managing ERP data risks.

At the beginning of 2020, we surveyed senior decision-makers that use SAP in large enterprise organizations with a minimum of 3,000 employees or $1 billion in annual revenue.

Our goal was to gain a better understanding of how organizations are evolving their ERP security and risk management practices, the kinds of risks they're most concerned about, and how they view and prioritize user and system visibility, access control, oversight, and accountability.

These are our findings:

APPSIAN

Key Takeaways

1. **Business Process Risks Are Slipping Through the Cracks**
   Executive confidence is wavering in an organization's ability to detect business risks from fraud, theft, and human error. While concern is generally high, a lack of consistent visibility into these business processes highlights a gap that many have yet to address.

2. **IT Leaders Are Concerned About Excessive User Privileges**
   Excessive user privileges continue to be a top concern of leadership – and for good reason. Users have the keys to your kingdom, and with this, pose a heightened risk if their accounts are compromised or if they engage in malicious activity.

3. **Misalignment is Hurting Confidence in SAP Security**
   Tight alignment between SAP security controls and business goals and objectives is paramount to secure, compliant, and efficient business processes. However, many respondents signal that the two are not aligned effectively.

4. **Limited Visibility & Complex Controls Are Hindering Progress**
   Organizations are facing the limitations of their existing technology and processes. Solving this will require a new approach to overcome complexities in controls and limited visibility into their business-critical applications.

APPSIAN

#1

Business Process Risks Slipping Through the Cracks

Only 17% of senior stakeholders are "very confident" in their organization's ability to detect fraud, theft, and error within their SAP business transactions. A leading cause for these types of violations is weaknesses in internal controls; specifically, misalignment of IT controls to business rules and objectives. Only 1 in 5 organizations are reviewing role and privilege alignment on a continuous to quarterly basis – while 26% of respondents have not in over a year.

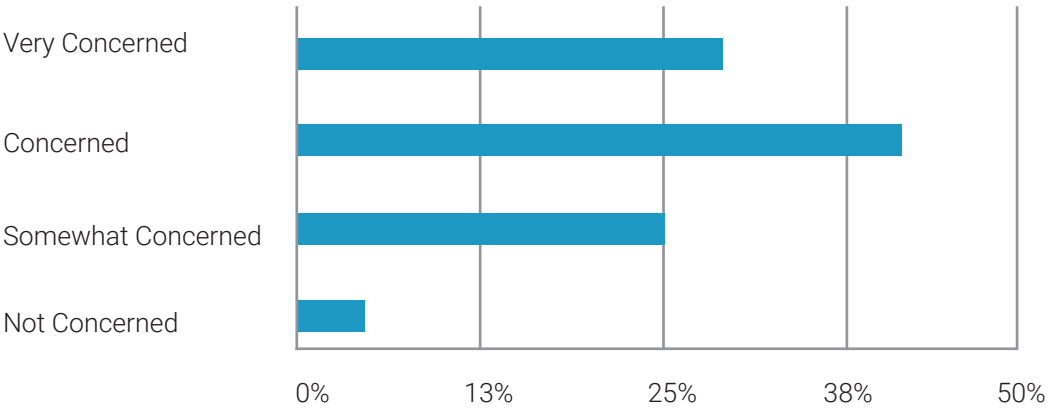
19% Audited within the past < 3 months

26% Audited 12+ months ago

Visibility into user activity, policy violations, and role and privilege utilization is the first step in identifying control weaknesses. Organizations that review this information on a more regular basis reduce the risk of violations going unnoticed and can realize a bottom-line cost savings by remediating risks before they balloon into a larger problem.

Does the C-Suite Care?

Q: "How concerned about mitigating business risks in SAP ERP transactions are your C-level executives?"



APPSIAN

#2

IT Leaders Are Concerned About Excessive User Privileges

66% of respondents were either "very concerned" (19%) or "concerned" (47%) about excessive user privileges. Managing roles and permission lists and keeping them current requires continuous vigilance. Ensuring users only have the minimum privileges needed to perform their duties, aligning to least privilege, allows an organization to reduce ERP access risks from unauthorized activity or unwanted data exposure.

Q: How concerned are you about excessive user privileges?

When asked to rate their level of concern about various ERP threats, respondents uncovered a pattern. The top three responses all correlate to user privileges being exploited by either an external hacker or the user themselves.

Q: "In relation to your SAP ERP applications, rate the following threats by your level of concern."

#1 Account Takeover (Phishing / Brute-force)

#2 Accidental Data Leakage

#3 Malicious Data Exfiltration

#3

Misalignment is Hurting Confidence in SAP Security

Only 1 in 5 respondents (21%) believe their role-based SAP security controls are strongly aligned with business stakeholder goals and objectives. Tight alignment between SAP security controls and business goals and objectives is paramount to secure, compliant, and efficient business processes. However, many respondents signal that the two are not aligned as well as they should be.

As gaps in alignment occur, doors open to invite additional threats. And these risks are acknowledged by senior leadership, with 70% expressing heightened concern on the topic and 54% ranking business process control enhancements as their top priority for the year.

What is Your Top SAP Security and Compliance Concern Headed Into 2020?

*This survey was administered before COVID-19 had its widespread impact. Response #2 has likely gained priority due to these circumstances.

#1 Managing Roles and Privileges in Service to Segregation of Duties (46%)

#2 Managing External Access in a Dynamic Environment (25%)*

#3 Enhancing SAP to Address Growing Compliance Risks (19%)

APPSIAN

#4

Limited Visibility and Complex Controls Are Hindering Progress

As organizations move to adapt to changing threats and business requirements, it is becoming clear that existing technologies and processes are reaching their limitations. Especially when it comes to an organizations' ability to understand data access, along with their usage of roles and privileges. While business objectives demand a clear line of sight into ERP activity, senior leaders have expressed deep concerns into their ability to remain aligned.

When asked to rank ERP access control challenges, the top three results were:

1. Lack of Granular Visibility into Role and Privilege Utilization
2. Ongoing Complexity with Role Provisioning
3. Static Roles Determining Access in Dynamic Environments

Complex controls are stifling organizations' ability to respond quickly and limiting the scope of risk that can be addressed with finite resources. Limited visibility, whether it be due to a lack of granular insight or extended gaps between reporting periods, compounds the problem as identifying deficiencies is the first step towards improving controls.

As mentioned in the previous section, **only 1 in 5 organizations are regularly auditing roles and privileges** on a quarterly to real-time basis. For broader reviews such as an IT General Controls audit, **48% are performed on an annual cadence,** with the remaining respondents citing 26% bi-annual and 22% quarterly periods.

Q: "Do you feel that your organization has enough visibility into SAP data access to proactively mitigate threats?"

APPSIAN

Conclusion

Executives who are seeking to enhance their enterprise risk management strategies are finding roadblocks and blind spots throughout their ERP applications. As business becomes more complex and ERP access more ubiquitous, gaining a holistic view of how users are interacting with high-risk data and business processes is becoming a bigger priority.

While heightened visibility is a prerequisite in improving risk management, complex controls must also be addressed to efficiently scale remediation. Without improvements in this area, organizations will be limited by the scope of risk that can be mitigated with finite resources.

Organizations with the most mature enterprise risk management strategies are seeking ways to prevent risk rather than react to risk. Having continuous visibility into their environment with routine audits, data access monitoring, and leveraging automation will help in this endeavor. Further evaluation of controls across business functions and how these controls are interconnected with their levels of risk are all considered best practices.

APPSIAN

About Appsian

Appsian Security Platform (ASP) enables organizations to fill critical data security and compliance gaps in ERP applications like SAP ECC and S/4HANA. As a native bolt-on solution, ASP delivers a comprehensive suite of fine-grained, risk-aware access controls along with continuous monitoring and analytics capabilities designed to proactively detect potential business risks.

For more information, please visit www.appsian.com

APPSIAN

8111 Lyndon B Johnson Fwy. Dallas, TX 75251

+1 (469) 906-2100

info@appsian.com