SafePaaS™

Essential Buyer's Guide
for a Segregation of Duties Solution

Segregation of Duties Buyer's Guide

Regardless of size or industry, most businesses have some core business application or ERP system that needs Segregation of Duty (SoD). SoD ensures proper oversight and reduces the risk of fraud or data breaches within your core system.

Segregation of Duties poses a distinct challenge, requiring strong collaboration between business and IT stakeholders to evaluate, mitigate, reduce, and monitor cyber, fraud, and material misstatement risks. Consequently, the implementation of SoD relies on software solutions since manual controls, whether managed internally or by consultants, often lack the robustness necessary to address the intricate nature of modern IT environments.

In this Segregation of Duties Buyer's Guide, we will discuss the far-reaching impact of SoD on various aspects of your organization's operations and the features and functions required to meet the challenge. Whether you are a dedicated compliance officer striving to meet regulatory standards, a CIO vigilant about safeguarding against cybersecurity threats, a meticulous financial controller responsible for internal controls, or a leader seeking to increase innovation while managing risk, this guide will be valuable in your decision-making process.

Segregation of Duties: Why is it so Complicated?

Enterprise applications, like SAP, Oracle, and Microsoft Dynamics, help your organization manage and streamline processes and automate operations. This reality has turned SoD into a matter of access control because almost all accounting and finance operations are carried out in digital systems. And ineffective Segregation of Duty access control within your ERP can result in operational losses, financial misstatements, breaches, and fraud.

Access Governance solutions have become essential for organizations to effectively manage SoD and to control role changes and user responsibilities. Access governance solutions are crucial in continuously recalibrating your Segregation of Duties protocols to safeguard against internal risks. Without the right solution, managing this process becomes complicated, time-consuming, and often quickly outdated due to constantly changing system access needs.

Typically, organizations resort to a mix of spreadsheets and SQL to fulfill auditor requirements, imposing an additional burden on already busy technical staff. However, this approach tends to yield inaccurate results, primarily because of the challenges in thoroughly analyzing every conceivable access route. Consequently, it frequently fails to detect users with access permissions that breach your SoD policies. Without an automated solution to verify potential SoD conflicts during access provisioning, it becomes unfeasible to guarantee that you are not unintentionally introducing fresh vulnerabilities.

SafePaaS™

The Intersection of Roles and Segregation of Duties

ERP systems are essential for organizations. They provide centralized control over critical business functions by enforcing user roles that execute SoD policies. But it is important to understand the intricacies of ERP roles to understand the requirements of an SoD solution fully. Below are the critical considerations and challenges posed by the interplay of ERP roles and SoD management.

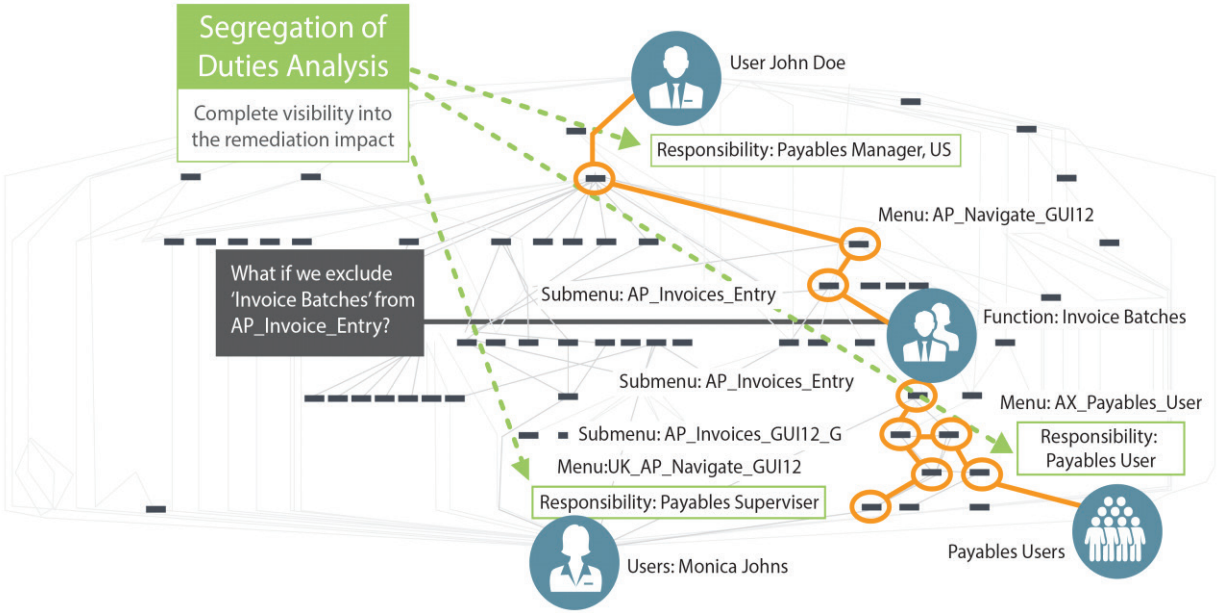
ERP SYSTEM ROLES AND SOD MANAGEMENT

ERP systems utilize roles to efficiently manage and restrict user access, enforce Segregation of Duties policies, automate processes, and uphold security and compliance standards. These roles are integral to access governance, ensuring users can carry out their responsibilities effectively while adhering to organizational policies.

VARIABILITY IN ERP ROLES

The specific ERP roles used can vary depending on your organization's requirements, industry, and the ERP system you use. However, certain default ERP roles are commonly encountered across different organizations, including:

- Administrator
- Manager/Supervisor
- Accountant/Financial Analyst
- Sales Representative
- Order Entry Clerk
- Purchasing/Procurement
- IT Administrator
- Customer Support/Service Representative
- Compliance Officer/Auditor
- Business Analyst
- Accounts Payable/Payables Manager
- Warehouse/Inventory Manager



CHALLENGES WITH DEFAULT ERP ROLES

Default or "seeded roles" in your ERP system can pose risks due to their configurations, which may not be specifically designed to prevent SoD violations. In some cases, these roles may contain inherent violations, requiring customization to align with your organization's compliance needs.

VISIBILITY AND SOD MANAGEMENT

Managers tasked with SoD management often encounter challenges in obtaining accurate lists and visibility into who has access to specific functions within your organization's applications. This lack of visibility can make it difficult to ensure employees are not engaged in conflicting tasks that could lead to compliance and security issues.

SOD RISKS IN USER ACCESS PROVISIONING

The process of user access provisioning introduces further SoD risks within your applications. IT Service Management (ITSM) and Identity Management (IDM) tools, such as ServiceNow, BMC Remedy, Microsoft Entra ID, Okta, and SailPoint, do not inherently control SoD risks at a granular level. These tools operate at a higher level and may not have the sophistication to detect privilege-level SoD issues. Additionally, they may not identify or prevent SoD violations in user access request workflows, which are crucial for compliance reporting, auditing, and forensics.

THE COMPLEXITY OF SOD IMPLEMENTATION WITHIN ERP SYSTEMS

Implementing effective SoD controls within your ERP system can be challenging, primarily due to the intricate and diverse nature of software applications that automate vital business processes. Ensuring ownership and accountability for managing these processes requires comprehensively examining the various functions available across different user roles and responsibilities. For example, evaluating SoD risk in an Accounts Payable application, where a user with the Payables Manager role can create suppliers and approve payments, demands a thorough analysis of all privileges associated with that role. It also requires distinguishing false positives stemming from factors like overridden settings, profiles, page-level configurations, or customizations that may restrict such access.

SafePaaS™

What Features and Functions to Look for in a Segregation of Duties Solution

POLICY DEFINITIONS – RULES MANAGEMENT

As ERP vendors like Oracle evolve, your organization needs the ability to adapt to the changes seamlessly. If your security model isn't configurable, you may find yourself with a dead-end SoD solution.

For example, Oracle GRC was once a viable solution but stopped being fully supported and lacked configurability. This limitation made using the same model for Oracle ERP Cloud impossible. Hence, the ability to configure your security model is essential to ensure the longevity and effectiveness of your solution.

Policy definitions and rules management are the foundation of any SoD solution. These features allow your organization to define and manage specific policies and rules that govern user access and actions within your ERP. The significance of this feature cannot be overstated, as it forms the basis for identifying and preventing potential conflicts. With policy definitions and a rules management capability, your organization can:

- **Define Policies:** Establish clear and comprehensive policies that outline which combinations of access and actions are restricted. These policies typically contain various aspects of an ERP system, including financial transactions, data access, and user roles.
- **Customize Rules:** The ability to tailor rules to suit your ERP environment's unique requirements and configurations. Different organizations may have different definitions of what constitutes an SoD violation based on their business processes.
- **Update Policies:** Adapt policies and rules to acommodate your evolving business needs and regulatory changes. As ERP systems and business processes evolve, the ability to modify policies is essential to ensure continued compliance.

SafePaaS™

ERP Security Model Configuration

A key capability is a SoD solution that works with your current technology and can evolve as your technology changes. This adaptability is crucial in preventing security risks in your changing environment.

The dynamic nature of technology and the shift toward cloud-based solutions requires a highly configurable security model. Here's why this feature is crucial:

- **Adaptability:** As ERP vendors like Oracle continuously introduce updates and new features, organizations must ensure that their security model aligns with these changes. Failure to do so can result in security gaps and compliance issues.
- **Compatibility:** A configurable security model ensures compatibility with different ERP versions and deployment options, such as on-premises and cloud-based solutions. This flexibility prevents organizations from getting locked into a dead-end security solution.

Snapshot Security Objects from ERP

Another vital aspect of an SoD solution is effectively monitoring changes. Snapshot security involves assigning users to roles and ensuring completeness and accuracy. With regulations like the PCAOB (Public Company Accounting Oversight Board) guidelines gaining importance, the ability to extract and provide evidence accurately is critical.

Snapshot security, or the ability to monitor changes, is essential for maintaining a secure environment. This feature involves continuously reviewing and validating user-role assignments and security objects. Here's why it matters:

- **Completeness and Accuracy:** Ensuring that user-role assignments are accurate and complete is critical for preventing unauthorized access and security breaches. The ability to provide evidence of the accuracy of these assignments is vital for compliance with regulations and PCOB guidelines.
- **Regulatory Compliance:** Regulatory bodies require organizations to demonstrate the accuracy and completeness of their security controls. Snapshot security helps organizations meet these compliance requirements by providing a reliable way to extract and validate security data.

SafePaaS™

Testing User and Role Assignment - Scoping

Testing is an integral part of ensuring the effectiveness of your SoD solution. Testing for Segregation of Duties policy violations, user-role assignments, and security objects is important. However, not all tests are created equal.

Buyers should inquire about the speed and frequency of Testing. Some solutions may take an excessively long time to process tests, which can hinder efficiency. Understanding how Testing aligns with your organization's data volumes and requirements is essential.

Furthermore, the ability to filter and scope tests is critical. Testing should allow you to focus on high-risk areas and specific business units where policies must be enforced.

ERP systems may support multiple security models, and your SoD solution should be flexible enough to accommodate these variations. For example, some ERP systems use roles and permissions, while others rely on different methods for granting access to users. For example, the Oracle E-Business Suite security model can be configured to grant users access based on Responsibilities and Roles, where roles are managed through User Management (UMX) HTML pages.

Inherited risk is another consideration. Users may inherit risk through roles in ERP systems like Oracle ERP Cloud and Workday. Testing should be flexible enough to address these nuances. Testing allows your organization to identify and remediate SoD policy violations, user-role assignments, and security objects. Here are the key aspects of testing:

- **Speed and Frequency:** Your organization needs to assess the speed and frequency of testing. Slow testing processes can hinder efficiency and delay critical risk identification and mitigation.
- **Scoping:** Scoping refers to the ability to focus testing efforts on specific high-risk areas and business units within your system. This granularity allows your organization to prioritize testing efforts based on the areas that pose the greatest risk.
- **Flexibility:** ERP systems may employ different security models and methodologies for access control. A flexible testing framework should be capable of accommodating these variations and nuances in security configurations.
- **Inherited Ri::** In some ERP systems, users may inherit risk through duty roles or other mechanisms. Effective testing should be flexible enough to accurately identify and assess these inherited risks.

SafePaaS™

Managing False positives

One of the critical features of segregation of duties software is its ability to manage false positives effectively. False positives can be a significant challenge in any security or compliance system, and in the context of ERP environments, they can create unnecessary work for your organization.

UNDERSTANDING FALSE POSITIVES

False positives occur when your system wrongly identifies an activity or event as an SoD violation; in reality, it isn't. These false alarms can lead to various problems, including wasted time and resources spent investigating non-issues and unnecessary disruptions to business operations.

SafePaaS™

ERP-Specific Nuances

In the context of ERP systems, false positives can be particularly challenging. ERP systems are complex and highly customized to meet an organization's unique needs. As a result, they often have ERP-specific nuances that can trigger false positives. These nuances may include:

Inter-organizational Risks: In some ERP configurations, inter-organizational risks may be flagged as violations when, in reality, they are not risks at all. For example, transactions between different business units or entities may be a common and legitimate practice in organizations with shared service centers. However, a less sophisticated SoD solution might flag these transactions as violations.

Inherited Permissions: ERP systems often use roles and permissions to manage user access. However, users may inherit permissions from higher-level roles. If not properly accounted for, this inheritance can lead to false positives. For example, a user with access to a broad role may have inherited permissions for specific tasks, leading the system to incorrectly flag potential conflicts of interest.

Complex Workflow: ERP systems typically involve complex workflow processes. False positives can arise when the system does not accurately understand the intricacies of these workflows. For example, a user may need temporary elevated permissions to complete a specific task within a defined workflow, which can be mistakenly flagged as a violation. Effective SoD solutions recognize the complexity of ERP environments and provide tools to mitigate false positives. Here's how it can help:

Granular Configuration: A strong SoD solution allows your organization to configure rules and policies at a granular level. This means tailoring the system to the specific nuances of your ERP setup. By customizing the rules, organizations can reduce the likelihood of false positives triggered by legitimate actions.

Contextual Analysis: Instead of relying solely on predefined rules, advanced SoD solutions can perform contextual analysis. These solutions consider the broader context of user actions and transactions, distinguishing between regular operations and actual violations. This contextual awareness significantly reduces false positives.

Filtering Capabilities: SoD solutions should offer sophisticated filtering options, allowing your organization to categorize and prioritize alerts. This way, high-risk alerts receive immediate attention, while less critical ones can be reviewed later, reducing the workload associated with false positives.

SafePaaS™

Roles Design and User Request Management

Role management is crucial in preventing access conflicts and ensures the creation of roles free from Segregation of Duties (SoD) conflicts. Organizations must exercise caution during the initial design and assignment of roles and during periodic reviews. These reviews are essential to identify any unauthorized changes, the accumulation of access rights, and the proliferation of roles over time.

Effective role management practices allow role owners and system administrators to establish and maintain consistent, conflict-free roles throughout the organization's systems. The role management provided by SoD control monitoring tools extends to roles managed within applications that incorporate their role management frameworks into their authorization models.

Role simulation capabilities enable administrators and role owners to conduct "what if" analyses at various stages of a role's lifecycle management. This functionality supports compliant user provisioning and ensures that SoD conflicts are proactively managed.

ACCESS CONTROL AND CERTIFICATION

Access control and certification are crucial capabilities when buying a segregation of duties (SoD) solution because they directly address security and compliance concerns within your organization.

Here's why they are important:

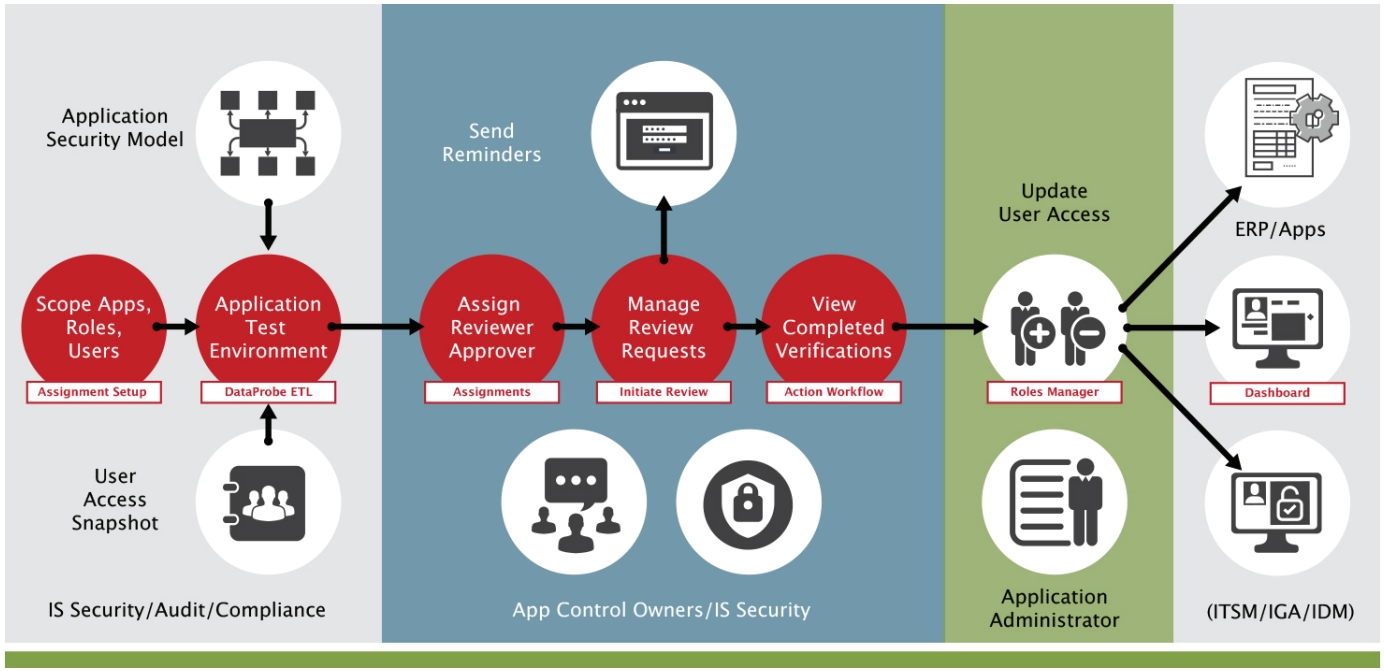
Reduce the cost of SoD compliance: Access controls and certification reduce the costly burden of SoD remediation by certifying role assignments before launching an SoD test. Customers that don't certify identities before testing segregation of duties risks get overburdened with the analysis and remediation of SoD risk that could easily have been removed through the termination of role assignments that are no longer active.

Preventing Access Control Failures: Access control failures can lead to unauthorized access to sensitive data and systems, resulting in breaches, compliance violations, and financial losses. An SoD solution helps ensure that only authorized individuals can access resources by automating the access certification process. This reduces the risk of human error and oversight in managing your access permissions.

SafePaaS™

Comprehensive Coverage: The SoD solution should cover all identities across various data sources, including identity management (IDM), identity governance and administration (IGA), IT service management (ITSM), databases, infrastructure, and servers. This comprehensive coverage ensures no critical access permissions are overlooked during certification, enhancing your organization's security posture.

Access Revocation and Role Adjustments: Automation of access revocation and temporary role adjustments are essential for promptly responding to security incidents, employee departures, or role changes. Delays can be risky when someone's access needs to be revoked or adjusted. An effective SoD solution allows quick and automated changes to be made, minimizing security gaps and potential breaches.



SafePaaS™

Scalability

Adaptation to Change: Your organization is dynamic and constantly developing. Change occurs when you adopt new technologies, upgrade systems, modify business processes, or restructure. In such scenarios, your SoD controls must be flexible and adaptable to accommodate these changes seamlessly. A rigid or static SoD solution may fail to address your evolving security needs.

Integration with New Applications: As new applications and technologies are introduced into your organization, they must be integrated into your SoD controls to ensure consistent security and compliance. A scalable solution should be able to integrate with these new applications without causing disruptions or delays.

Long-Term Sustainability: An SoD solution that can scale with your business provides a sustainable approach to managing security and compliance. It avoids constant replacement and reimplementation, which can be costly and time-consuming. Instead, it grows with your organization, offering long-term value and effectiveness.

To learn more about how SafePaaS can help your organization with Segregation of Duties please, **contact us**.

3300, Dallas Parkway, Suite 200, Plano, Texas, 75093 USA

SafePaaS™