MOSSADAMS

WHITE PAPER

Segregation of Duties: Best Practices for Cybersecurity and More

The news is filled with stories of alarming cybersecurity breaches, networks being hacked, and malware running amok. However, there's another, less obvious, yet equally insidious, cybersecurity risk lurking inside just about every organization: inadequate segregation of duties (SOD).

SOD suggests that problems—such as fraud, material misstatement, and financial statement manipulation—have the potential to arise when the same individual is allowed to execute two or more conflicting sensitive transactions. In today's business environment, SOD is often synonymous with IT system access rights because the majority of critical functions are performed through enterprise systems.

Inappropriate SOD is often the root of many significant internal control problems. The pace of business-technology change continues to accelerate and underpin more of our daily business processes. Unfortunately, fraud risks are evolving along with technology as innovative business software creates more opportunities to commit fraud.

For example, while cloud-based enterprise resource planning (ERP) systems have led to increased business efficiency and flexibility, they also present a heightened security risk that requires stronger access controls. Performing a regular SOD analysis can help mitigate some of this risk.

WHY IT MATTERS

SOD problems within an ERP system can serve as a proverbial iceberg, with much of the risk lurking out of sight. Often, there's an assumption that SOD was fully considered as part of system implementation because it's a fundamental business practice, but this isn't always the case. It takes a strong, targeted effort to unearth the gaps and deficiencies left unnoticed or unresolved.

If there's more than one application in an environment, which is the case for almost every organization, it's almost assured that interapplication risks haven't been considered.

Many organizations discover serious risk exposure when they roll out the access security and monitoring modules that have recently implemented governance, risk, and compliance (GRC) software suites, indicating that past confidence in SOD may have been misplaced.

The power of SOD isn't often fully appreciated, and consequently it's viewed as having the same priority as other transaction-level internal controls. As a result, system access rights are poorly designed and SOD isn't used effectively.

However, appropriate SOD enforced by an ERP security system is one of a handful of foundational controls. By working to establish appropriate SOD, organizations can significantly improve their risk management capabilities.

KEY ISSUES

Managing system-enforced SOD in a pragmatic, effective way is more difficult than it seems. The complexity of today's enterprise systems leaves many companies struggling with a number of SOD-related issues.

Role-Based Security

Modern-day ERP systems often rely on role-based security, which theoretically simplifies security administration; however, the design of roles is often inappropriate. This risk is further compounded by the fact that there's frequently more than one way to perform a function or access data within a modern ERP system.

Accountability and Oversight

A lack of oversight and clear accountability for system access rights can create issues. Because these system-enforced access controls rely on IT systems to operate, they're often erroneously considered IT controls. Even though an IT department may manage the technological aspects, SOD is still a business control.

The IT department often handles the technical administration—grants rights, removes access, and changes access, for example—but it's the business owners who define what's appropriate. Because SOD requires this level of technical and policy coordination, it can often fall through the cracks.

FIXING ISSUES

Appropriate SOD can often be viewed as a Gordian knot in the context of a large and established ERP system, where untying it is deemed impossible because of the potential disruption to day-to-day operations. A systematic, rational, and risk-based approach can go a long way in fixing—or at least acknowledging and compensating for—SOD issues without causing too much of an unwelcome disruption to daily business processes.

Holistic Approach

An SOD analysis needs to be holistic and not piecemeal. A common mistake when assessing SOD is running security reports with limited data and manually assessing appropriate access and duty segregation. This limited approach is error prone because modern ERPs have many different methods for processing

transactions, and the number of potential conflicts often numbers in the tens of thousands.

A better approach is to extract all security configurations—user access rights and role configuration, for example—and analyze them through a relational database. Many off-the-shelf systems exist to facilitate this process, with a large number emerging in the past few years as more software vendors offer ways to automate the process. Depending on the application, these tools can be built into the application or offered as a third-party module, stand-alone application, or cloud-based service.

Much of the up-front work involved in this approach is still required, but these software solutions can help significantly streamline the actual analysis and administration of an SOD analysis.

Risk-Based Approach

The second critical aspect of an effective SOD analysis and remediation is a risk-based approach. There are many potential exposures in ERP systems, but not all SOD conflicts are of equal importance.

Segregated Activities

- Transaction initiation
- Authorization
- Asset custody
- Recording
- Reporting
- Reconciliation

Some of the above activities are more likely than others to lead to material fraud or financial statement issues if not properly segregated. That's why an SOD analysis and remediation process need to be prioritized based on issue probability and impact, with a consideration for cost.

SOD REVIEW PROCESS

Although specifics may vary due to the security model employed, a general process or framework can and should be followed to help SOD review results be as complete and consistent as possible.

General Framework

- Understand the security model employed
- Determine analysis approach
- Link key activities and SOD rules to system permissions
- Perform the analysis
- Address conflicts

The above model focuses on business process SOD.

Within the IT function, there's also a need for adequately segregated duties. Although the general principles are the same, the process, terminologies, and risks are different. For example, the employees developing and testing software changes shouldn't also be putting the software into production.

It's highly advisable that organizations also consider the appropriate SOD within their IT processes.

STEP ONE: UNDERSTAND THE SECURITY MODEL EMPLOYED

The type of underlying system that's being reviewed can have a dramatic effect on what's considered and how the SOD analysis itself is structured. It's also important to understand the security model employed by the application being assessed because this can help to determine how SOD conflicts should be identified and addressed during a formal analysis.

For example, if an organization only considers access to roles or to t-codes during an SOD analysis of SAP, false positives are possible whenever access is granted through authorization objects. Customized changes to a purchased application can also affect what and how access rights are analyzed.

Application security is generally based on one of two basic concepts:

- **View permissions**—restrict the windows shown to users
- **Logical permissions**—restrict the read/write access to specific data tables or fields

Logical permissions are often applied to user accounts in bundled groups called roles or profiles. Different

applications may allow one or multiple roles or profiles to be applied to user accounts, which can often be customized and include conflicts within a single profile.

STEP TWO: DETERMINE ANALYSIS APPROACH

It's critical to gain a clear sense of an organization's business processes by defining what activities or functions are key and should be appropriately segregated. This is why the overall objective of this step is to develop a complete list of key activities and an understanding of which of those activities conflict.

A more complete list of key activities and duties will help facilitate a stronger SOD analysis. By including a brief description of any relevant activities as well as the risk related to each conflict, organizations can also help ensure an analysis is usable in the future. It's important to note that key activities and the SOD rule set don't need to be specific to the functionality within the system being analyzed during this step.

SAMPLE: GENERIC KEY ACTIVITIES

SENSITIVE ACTIVITIES	Customer master	Sales order entry/edit	Sales order approval	Ship confirm	Vendor master	Requisition entry/edit	Requisition approval	Purchase order entry/exit	Purchase order approval	Receiving	Inventory adjustment entry
Customer master	■	▒									
Sales order entry/edit	▒	■	▒	▒							
Sales order approval		▒	■								
Ship confirm		▒		■	▒						
Vendor master				▒	■						
Requisition entry/edit						■	▒				
Requisition approval						▒	■				
Purchase order entry/edit					▒			■	▒	▒	
Purchase order approval								▒	■		
Receiving						▒		▒		■	▒
Inventory adjustment entry				▒						▒	■

▒ Conflicts ■ Duplicate functions

Many generic SOD rule sets, such as the example provided above, are widely available and a great place to start when defining key activities to test during an SOD analysis. There are also rule sets geared toward various ERP systems, including SAP, Oracle, and NetSuite.

An organization can customize these rule sets as needed. An effective and efficient way to do so is to use existing process documentation, such as SOX or ISO. It's also important to look at risk-control matrices for any control descriptions that rely on restricted access to work effectively.

STEP THREE: LINK KEY ACTIVITIES AND SOD RULES TO SYSTEM PERMISSIONS

Once an organization has defined the key activities in each business process and identified relevant conflicts, it's time to translate those generic activities into the specific security details of the organization's ERP system.

This is probably the most difficult step in the analysis. Unless an organization uses an SOD analysis tool, a business analyst or IT administrator may need to assist with linking each discrete business activity to the related security object that allows users to perform said activity.

Even if an organization uses an SOD tool geared toward its ERP system, the organization still needs to work with an analyst or IT administrator to account for customizations. This is because many organizations have business processes and activities that are unique enough that they need to be defined from scratch. In SAP, for example, Z-transaction codes are custom developed, which means they need to be specifically considered in an SOD rule set.

Defining System Permissions and Security Access

The granular system permissions that allow key activities need to be identified and mapped to each activity. These permissions can be defined and described as whatever is the most basic security unit that a user account would need to access the key activity, such as:

- Menus
- Screens
- Fields
- Transaction IDs
- Authorization objects

A number of discrete permissions and granular security access may grant access to a single key business activity. Working with a business analysis or application specialist can help an organization better understand what does what. A specialized SOD or GRC tool can make this process easier, but the mapping will still need to verified if an organization uses any custom activities or security measures.

Mapping Security Access

Many SOD conflicts are due to poorly designed roles that grant conflicting granular access in a single role. As such, focusing on the granular attributions that an application requires of a user account to perform a key activity is often more useful during an SOD analysis.

Mapping granular security access may not be enough because this type of access can be configured to limit its capabilities, such as:

- Read-only access
- Certain transaction constraints
- Certain business unit restrictions

If these additional configurations aren't considered, it's likely that any SOD analysis will yield false positives that incorrectly suggest conflict exists. In addition to undertaking these considerations, an organization should review for completeness and reasonableness the final list of target SOD conflicts and mapped system permissions.

Exclusion of Manual Activities and Security Roles

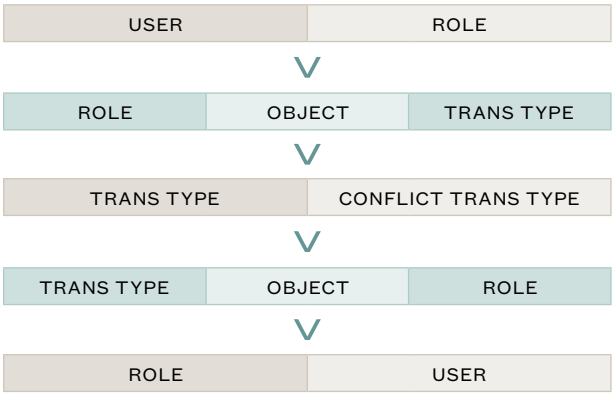
The complexity of an organization's ERP will determine how many identified activities are purely manual activities—in other words, activities that require no system interaction. For the purposes of this analysis and discussion, the consideration of manual activities has been excluded. However, as an organization improves its SOD compliance, it'll be important to factor in the activities done outside the system.

An SOD analysis also shouldn't be performed with security roles, which are groupings of granular security accesses related to a job function. While these roles are useful for administering security, they can cause confusion during an SOD analysis focused on business processes because the roles aren't descriptive enough to understand what permissions have been granted.

STEP FOUR: PERFORM THE ANALYSIS

Once permissions and activities have been linked, permissions-based conflict pairs can be created—in other words, an organization can identify SOD conflicts. If an organization isn't using an SOD or GRC tool, it needs to develop a relational database to effectively execute the pairwise comparisons.

The underlying logic of the analysis allows any single user to compare his or her access rights against the table of predefined conflicting key activities. Any time a user has both sides of a conflict pairing, an SOD violation exists.



Once a concrete framework, or standard, has been defined, permissions associated with users and roles should be exported from the application and compared to the standard to identify any SOD conflicts that have resulted from an improperly designed single role or a user with multiple roles.

STEP FIVE: ADDRESS CONFLICTS

An initial SOD analysis is often shocking because it uncovers security issues that weren't previously visible or known—especially if the security and SOD considerations taken when implementing the ERP system were less than ideal. Examples include the following:

- Roles were established by software implementers with little consideration of formal SOD.
- Security may have been one of the last considerations in the implementation process and therefore rushed due to an impending go-live date.
- Organizational personnel moves within a company often result in employees collecting access rights because new rights are requested for each new position without old access rights being removed.

Once the analysis is complete, organizations will want to take a measured approach to remediation. Each SOD conflict has its own risk profile, which makes ranking each type of conflict critical. This enables organizations to prioritize their efforts on the areas with the highest likelihood or impact.

False Positives

It's likely that false positives will be identified in the initial analysis. Testing conflicts to help verify that the results are accurate is an important next step. Once confirmed, organizations can benefit from understanding what's driving false positives—such as additional limitations and configurations at the permission level—and reanalyzing the data accordingly.

This iterative approach can help organizations further refine and prioritize conflict areas needing remediation. At a minimum, false-positive results cause unnecessary alarm and require time to confirm. In worst-case situations, false positives can lead to unnecessary changes to user access rights and business processes.

Common Conflicts

False positives aside, SOD issues result from users being assigned improperly designed roles—known as conflicts within roles—or through users being assigned multiple roles, known as conflict between roles.

Conflicts that are part of custom roles can be resolved by removing at least one side of the conflicting activity. For individual users with conflicting permissions or role combinations, a business assessment can identify if the conflicting access is necessary or if a compensating control can be identified or designed instead.

Conflict Resolution

Ideally, all conflicts can be addressed through redesigning roles or shutting down unneeded access. However, changes to business processes and personnel capabilities are often necessary because many conflicts are institutionalized within users' roles and responsibilities. This type of conflict resolution can take time.

It's important to thoroughly document resolutions to these issues—whatever the remediation process:

- Change role structure
- Remove user access
- Use compensating controls

Use existing processes, such as help desk tickets, to complete and approve actual system changes. This can help make sure an SOD analysis and improvement initiative don't create additional problems through poor change management.

For smaller companies, there may not be enough qualified personnel to adequately segregate duties, and the benefits of strong SOD may not appear to justify the cost of hiring additional personnel.

Whatever the reason for imperfect SOD, there are alternative approaches. Organizations that understand the risk created by conflict are often able to create compensating detective and preventive controls that can mitigate risk through oversight and monitoring. For example, if SOD within an organization's procurement process isn't possible, a robust bank reconciliation may be able to mitigate the risk of inappropriate or fraudulent purchasing when performed by an independent and qualified person.

SOD Analysis Frequency

An SOD analysis is a business control, which means the business—not the IT department—is responsible for ensuring it's performed periodically. There's no right or wrong answer to how often a review should be performed.

For example, an organization with an annual compliance need has to perform an SOD analysis at least once per year while many organizations conduct an analysis more frequently, particularly in times of rapid change due to growth, layoffs, and organizational restructuring.

Historical results can be used to determine how often an assessment should be performed, with the more issues historically identified, the more likely a higher frequency of analysis is needed.

CONCLUSION

SOD is an often misunderstood and underestimated area of internal control, with many companies assuming they have no substantive issues. This assumption is rarely based on a system analysis but rather on a perceived lack of problems.

In reality, most companies experience significant SOD challenges. To truly understand the extent of an organization's SOD status, it's imperative a systematic and rational evaluation approach be used. Although maintaining strong SOD compliance can take time and effort, it's worth it because of how foundational SOD is to other business controls.

Learn More

If you'd like to learn more about how an SOD review could benefit your organization, contact your Moss Adams professional or visit **mossadams.com/SOD**.

About Moss Adams

With 2,900 professionals across 25-plus locations in the West and beyond, Moss Adams provides the world's most innovative companies with specialized accounting, consulting, and wealth management services to help them embrace emerging opportunity. Discover how Moss Adams is bringing more West to Business.