FINANCIAL CONTROLS

Automating risk management while implementing ERP

Effectively managing Segregation of Duties (SOD) is a key requirement for any enterprise resource planning (ERP) or financial system to pass an audit. Initiation and efficient maintenance of SOD requires a fully automated financial control testing platform to identify, prevent, and mitigate issues that can negatively impact the accuracy and validity of financial reporting—putting the organization at risk. Best practices recommend that SOD compliance become part of any initial ERP implementation or migration early in the process. The result is reliable, trusted security that also allows project teams to stay focused on mission-critical tasks.

Automation and risk avoidance

What is Segregation of Duties?

Segregation of Duties (SOD) requires organizations to ensure users of business applications do not have the capability to perform two processes that could permit fraud, waste, and abuse. These are called “toxic access combinations” and enable an individual to execute such fraudulent activities as creating and paying himself as a supplier. That is theft.

Competent, automated SOD policies will prevent users from being assigned these toxic combinations. Baker Tilly reports that “Among the various kinds of fraud that organizations might be faced with, occupational fraud is likely the largest and most prevalent threat today…causing organizations of all types and sizes to rethink their approach to governance, risk management, compliance, internal audit, and the design of their internal controls.”[1]

Proper SOD is an expected part of many financial auditing regulations, including:

- Sarbanes-Oxley (S/OX) in state/local, tribal, and commercial organizations
- OMB A-123 Internal Controls over Financial Reporting in Federal Civilian agencies
- Financial Improvement and Audit Readiness (FIAR) in the Department of Defense community
- Improper Payments Act (IPA)
- Federal Information Security Management Act (FISMA)
- Federal Financial Management Improvement Act (FFMIA)
- National Institute of Standards and Technology (NIST) 800-53 Access Controls (AC)

Experts say that simply maintaining a compliance program is not enough. Compliance programs and internal controls must be adequate and effective at preventing and detecting fraud. Moreover, recent enforcement actions highlight the importance to organizations that internal controls must be continuously monitored to ensure they are effective.[2]

Staying secure through implementation and upgrade

Understand the risk

Many organizations struggle to implement or upgrade their ERP and financial systems on schedule, given the complexity of those systems and the amount of configuration they require. That means proper access controls may not be a priority, which creates unacceptable—and often costly—risk.

Get clean, stay clean

SOD should be deployed as part of an integrated migration or new implementation of all business applications where toxic combinations expose an organization to fraud, waste and abuse. The concept of “get clean, stay clean” compels organizations to identify and mitigate all SOD issues before migrated or new applications are moved into production.

For new implementations, all business processes and roles should be planned and designed to prevent any potential SOD conflicts. Business process owners and IT teams are required to understand existing processes and design compliant flows to ensure the soundness of financial reporting. New systems should never be introduced with SOD issues, but should be designed to prevent any opportunity for fraud and abuse.

1. Jonathan T. Marks, "Combating Fraud Through Effective Internal Controls," January 19, 2019.
2. Ibid.

Prescriptive implementation strategies can be employed to utilize best practices in lieu of customization. Accelerators such as libraries of SOD controls provide an effective approach to streamline implementations, allowing for later adjustment in these automated controls if required.

For existing implementations, organizations should not simply re-deploy the same access and assignment policies from the current business application to its new platform. Without ensuring there are not any existing SOD issues, the same potential toxic combinations might be recreated in the new instance, thus exposing the organization's financial reporting to potential fraud. All modernization projects should ensure that the application of all financial controls is sound and effective.

Enforcing compliant user provisioning

Best practices

Typically, when organizations provision new users or support transfers of employees, out-of-date forms are completed and submitted to the IT team. Often, the forms are not understood by the managers requesting them. In most cases, the manager copies a form used for another team member who performs a similar role. This approach is fraught with opportunities for non-compliant provisioning and inadvertent assignments of toxic combinations and inappropriate roles.

New systems should never be introduced with SOD issues, but should be designed to prevent any opportunity for fraud and abuse.

Best practices for compliant provisioning require an automated approach to ensure all users, whether new hires or transferring employees, only have access to appropriate roles and access points. The same accelerators, or libraries of financial controls that are used to identify, prevent and mitigate SOD violations, should be deployed as part of the provisioning process. Generally, these rules can be executed as part of the verification and approval process, and can automatically flag users with toxic combinations. Before final provisioning can be completed, all SOD violations must be mitigated. Mitigation can be simply removing the toxic roles or applying automated compensating controls to monitor and restrict activities.

Another benefit to compliant provisioning is the ability to ensure all retiring or terminating employees are relieved of all roles within the organization's business application. Automatic notifications from human resource platforms should trigger de-provisioning of these employees' assignments, thereby eliminating any chance of financial malfeasance by departing team members.

Automating the attestation allows organizations to leverage the preventive SOD capabilities and assignments, and provide electronic notifications and sign-offs for all managers.

To complete required attestation of user roles, organizations often manually run reports, download to Excel®, and send emails requesting management approval of their employees' roles. Because this process is cumbersome, it seldom results in timely processing and deadlines are sometimes missed.

Leveraging an automated SOD tool to streamline this process eliminates the need to run reports and manually generate emails. Automation allows these activities to be scheduled, executed and monitored with minimal user interaction and within deadlines established by government rules.

High risk, high cost

Avoid costly mistakes

Experience shows that organizations spend more time, resources, and money to fix SOD issues after business applications have been deployed rather than preventing the issues up front. Organizations that design a SOD-compliant security model as part of the initial deployment can avoid costly security re-design efforts.

This is particularly critical for phased rollouts where SOD issues get multiplied through staged rollout phases if not addressed as part of the security design. In shared services organizations, the potential risks of not managing SOD further intensifies with the inherent complexity of managing multiple customers and systems with differing requirements.

"Segregation of Duties (SOD) is a basic building block of sustainable risk management and internal controls for a business. The principle of SOD is based on shared responsibilities of a key process that disperses the critical functions of that process to more than one person or department. Without this separation in key processes, fraud and error risks are far less manageable."

The American Institute of Certified Public Accountants (AICPA)[3]

Implementation partners who include SOD compliance in the initial rollout not only protect themselves from difficult conversations with their customers after go-live, they also protect their customers' limited resources from unnecessary fire drills by using their own staff to include a proactive strategy for effective and repeatable SOD management.

Finding value

Further, by using SOD automation tools, project teams can reduce time and risk. In contrast to running reports, manually checking for SOD violations, and redesigning roles, automated tools save the time and effort of ensuring compliance. Moreover, reports often do not provide a view into the access point of each role, so SOD violations may exist without being identified; in contrast, automated tools that understand the complex security and access models of each ERP ensure all violations are found.

Another area of savings involves streamlining provisioning activities. Rather than separate, manual processing of access requests, automated tools can automate the approval and provisioning of all users—again, saving time and effort by project teams.

3. AICPA, "Segregation of Duties,"

Deployments of SOD automation tools lend themselves to being run as a parallel and independent track to the main ERP deployment project. Qualified implementation partners with deep subject matter expertise in SOD deployments can take on the vast majority of the deployment efforts and need only minimal assistance from the core project team.

SOD as part of design

It's in the details

When roles are properly configured, SOD issues are identified as part of the design process. Implementation partners guide organizations through detailed analysis of business processes, owners, and tasks. Often, these design sessions parallel typical processes such as Procure-to-Pay, Order-to-Cash, general ledger and sensitive account processing, and more. Most automated financial controls platforms offer out-of-the-box libraries (also known as accelerators) designed to identify and prevent SOD issues. These best practices libraries should be leveraged as part of the role design to flag any potential compliance violations and allow an organization to confidently assign clean roles to users.

If preventing SOD issues is not part of the initial design and implementation, users who become proficient at their jobs may later find they lose critical access due to SOD violations. This results in frustration by the employees and broken business processes where tasks can no longer be completed. A user with an SOD violation will be restricted as their access points are revoked, and they will no longer be able to complete their jobs.

"As a former senior auditor with Ernst & Young, I always recommend leveraging solutions that provide continuous controls testing. These tools should be used as part of the user provisioning process, change control process, and role management process in the designing of new financial security roles so you can focus on other aspects of your deployment and not worry about these typical audit risks."

Emmanuel Twum, Vice President of ERP Advisory Services, New River Systems

Designating roles before deployment

Designing clean roles prior to the deployment of a business application ensures that employees will not have to be retrained when access becomes an SOD issue. Perhaps the most expensive issue related to post-implementation SOD deployment is an organization's exposure to audit findings. An SOD violation must be mitigated immediately. Organizations without an automated capability and who rely on running reports are often the ones most likely to experience fraud and abuse. Reports are often complex and unwieldly, and generally either too high-level to ensure SOD issues are found, or out of date within a day of execution.

Once an auditor finds an issue, the organization may receive additional scrutiny or, worse, negative publicity when fraud becomes apparent. Finally, organizations that must introduce new rules and guidelines into their provisioning processes are met with resistance. The hiring or transferring processes are designed to ensure users are on-boarded in an efficient, streamlined fashion. When these processes change to accommodate pre-assignment SOD validations, hiring managers and human resource teams are frustrated and have additional processes to review, redesign and reconfigure.

Saving time and money

SOD is a critical component to any organization's prevention of fraud, waste, and abuse. It's crucial that it be part of the risk management framework from the beginning of any ERP implementation and upgrade.

Whether the ERP system is being rolled out in phases or across the entire organization, a clean, SOD-compliant security model is essential for your organization to pass audits. Going live with noncompliant user access in phase one of a deployment quickly turns into a risk for subsequent rollout phases.

This approach is not only about avoiding negative consequences. Automated SOD capabilities and accelerators often provide additional benefits for organizations adopting a continuous controls monitoring approach to compliance. When SOD is enforced, compensating controls can be included to further mitigate the risk for fraud.

In some cases, and for a limited time frame, users are allowed to have toxic combinations to complete tasks. For example, a team member may be on leave so another member must perform their tasks. This may require a non-SOD compliant assignment. Automated solutions can monitor those activities and impose a threshold whereby a user may modify supplier records and also pay those suppliers, but all transactions that exceed a certain amount will be flagged for review. In this way, the organization provides another level of scrutiny when SOD situations must occur.

> **"Today's need for a proactive risk management-driven approach is changing the game; the trigger should be pulled at the earliest logical point and opportunity. The result will contribute to better risk management, a much lower cost of operation around keeping the access management clean, and far less costly interference by auditors and legislators."**
>
> **Hans van Nes**
> COO, Consider Solutions

Governmental guidelines require organizations to perform a quarterly (or periodic) attestation of all employees' roles and assignments. When SOD compliance is part of an implementation, managers can more easily attest that their team members' assignments are accurate and compliant, without worrying about violations.

Internal and external audits are expensive, manually-intensive, and often rely on only a sampling of SOD roles or transactions. In contrast, automated continuous controls-monitoring tools evaluate 100 percent of all role assignments and transactions that are processed by a business application. Compliance issues are flagged, assigned, and mitigated—and provide a detailed audit trail of all findings and resolutions. Auditors spend less time on testing financial controls because they are automated and less effort on overall financial audits.

As organizations rely more on continuous control testing of all roles and transactions, they have furthered their abilities to identify and prevent improper, fraudulent or erroneous payments. Just as automated tools provide a library of best practice SOD policies, they also offer best practice transaction and configuration monitoring. Duplicate payments, split POs, manual journals, vendor or bank account modifications, and other suspicious transactional activities are automatically flagged, assigned, and mitigated. Organizations may find potential issues before payments are made to avoid pay and chase processes that requires more time and effort to recoup lost financial assets.

Organizations save time and money while also elevating the audit to verify all roles and transactions.

Learn more ›

INF-2247125-en-US-1119-1