Minimizing fraud exposure with effective ERP segregation of duties controls

Prepared by:

Luke Leaon, Manager, RSM US LLP
luke.leaon@rsmus.com, +1 612 629 9072

Adam Harpool, Manager, RSM US LLP
adam.harpool@rsmus.com, +1 212 372 1773

November 2015

Fraud is a constant concern at every level of organizations, and many companies' control environments have failed to keep up; even the strongest reviews and reconciliations cannot completely reduce fraud, and significant exposures can occur at companies, regardless of revenue or number of employees. Advances in functionality and complexity in major enterprise resource planning (ERP) systems have further amplified the need for more attention to the design and monitoring of automated controls.

Companies must explore the risks around the lack of appropriate segregation of duties (SOD) controls which often enable fraudulent behavior. A poorly implemented SOD identification and mitigation process can negatively impact a company's ability to manage risks and prevent or detect fraud.

How SOD vulnerabilities occur

The main drivers of insufficient SOD controls are a lack of awareness or concern during the initial design and implementation of ERP system(s) and a lack of effective governance. In many cases, security and controls are an afterthought during an ERP implementation. It's rare to have an implementation team that also has significant experience with risk and controls.

When integrating complex ERP systems, key control points can be overlooked by implementers and business owners in lieu of deadlines, system usability, and simply getting the platform up and running. These factors can take precedence over carefully examining risks and undergoing a risk assessment to understand threats in major business processes, impacting choices on security and configuration, and who has access to what information.

Unprepared organizations typically must retrofit a control framework into their system following the identification of a compliance requirement or the discovery of a vulnerability or an incident; since these incidents tend to occur post go-live, they often must be addressed after organizations have lost key institutional knowledge from the original implementation team.

Making changes to a system after the implementation requires more effort and investment than if appropriate controls were included in the original design. Despite an ineffective implementation, companies can recover by implementing automated controls and placing more focus on monitoring controls, helping to establish effective SOD management and protect against fraud.

Limiting opportunity

The three key factors that enable fraud are pressure (also sometimes referred to as incentive), rationalization and opportunity. Pressure and rationalization are variables that are entirely independent of ERP or other technology controls. However, organizations can limit the opportunity to commit fraud by implementing effective internal controls, including ERP controls.

Strong top-down ERP SOD controls can effectively remove (or mitigate) the opportunity component of fraud. This level of ERP SOD requires a reexamination of the company's risk profile, typically through a broader lens than an audit, Sarbanes-Oxley assessment or other purely compliance-based concerns. In addition, this approach must involve diverse stakeholders, such as business process owners, internal audit, finance and IT. Importantly, this approach to ERP SOD also requires regular maintenance.

Common ERP security and SOD myths

Organizations struggle with several common misconceptions when managing the complexity of ERP systems. The following are common myths often at the root of SOD vulnerabilities:

- We have an ERP system with advanced security implemented by the vendor; therefore, SOD is not a major risk.
- We have a governance, risk and compliance (GRC) or continuous controls monitoring (CCM) tool with an industry-standard rule set; therefore SOD is not a major risk.
- Our ERP system is audited by both internal and external auditors each year, and we get clean audit reports. Therefore, we're not at risk.
- We have an SOD matrix to guide access provisioning; therefore, we're not at risk.
- We have many manual financial controls (e.g., account reconciliations), so our risks are mitigated.

The reality is that without a structured and continuous process to measure and mitigate SOD risk, a company's ERP control environment may facilitate fraud.

Developing effective SOD rules

To implement thorough SOD rules, a company must first identify key business cycles. A top-down approach should be taken, looking at business processes and determining key risks within these individual processes. Links should be created to subprocesses and specific activities.

Companies must evaluate the impact of the business processes they have (e.g., in terms of financial, operational and strategic importance), where they are performed, and whether they are performed within an IT system or as a combination of IT transactions and manual processing. They should then identify specific risks within each business activity at the most granular level possible.

When identifying each business activity, organizations must identify the key IT systems utilized to perform these functions. All IT systems involved in business processes should be evaluated for risk, including any cross-system processes and activities. Often, companies will evaluate their main system of record (such as an ERP platform) well, but overlook vulnerabilities in other interfaced systems that can occur across multiple processes and systems.

Many companies fail to perform that cross-system analysis; they may have a GRC tool connected to their ERP platform, but other access could result in fraud in other key systems. A common example is a company that utilizes a sophisticated ERP package such as SAP for the general ledger and financial reporting, while business functions such as inventory management remain within a legacy application. The proper cross-system SOD analysis would include not only SAP, but the attached legacy applications as well.

Finally, organizations must identify key controls, including SOD. These should include mitigating and compensating controls. The analysis should seek to determine whether key monitoring controls are performed by personnel who have transactional access.

Identification of SOD

After key business cycles have been identified and all activities are documented, companies must map them to corresponding IT systems or manual processes. SOD and sensitive access rules should be documented and examined periodically, with rules driven by degree of business risk. Any toxic relationships or potential opportunities for fraud should be identified and discussed from a risk and impact standpoint during this process.

A control around SOD is inherently two-sided, with a business activity that is in conflict with another activity. Sensitive access rules are driven by the inherent risk of having one business activity which is such a significant concern for an organization that it requires regular review and potential monitoring. Functions such as processing manual journal entries and certain system administrator rights are areas that may require periodic examination simply due to the nature of the business activity.

Common SOD conflicts

Companies often must resolve several conflicts when developing effective SOD controls. These can include:

- Cross business cycle access: For example, users with accounts payable invoice entry and payment access could pay an invalid invoice or fraudulent invoice.
- Initiate vs. approval: Within most business cycles, workflow approvals can be configured to verify that only authorized transactions are processed. If a user has access to both initiate and approve a transaction, this presents a segregation of duties issue and a potential opportunity to commit fraud.
- Transactional vs. reconcile: Individuals responsible for reconciliations (either manual or automated) should not have access to transactional functions which would effectively allow them to approve their own transactions in the ERP system.
- Develop vs. promote: Most ERP systems have custom development capabilities which allow enterprises to add new functionality to the system; typically, these changes are created in a development environment and "promoted" to the live production system once tested and approved. If users with access to develop changes can promote their own changes to production, they can alter system functionality without review and potentially perform fraudulent activity.
- Subsidiary vs. general ledger: Access to enter an invoice and enter a journal entry.
- Subsidiary general ledger vs. consolidate: Access to enter journal entries and cross-company adjustments.
- Business access vs. IT access: General leading practices suggest that IT access should be segregated from business end user access according to the principle of least access required to perform a job function. Granting users access to both business and IT functions can allow them to potentially circumvent controls designed to prevent fraud. (For example, users may be able to process fraudulent transactions—business access—and then delete the logs which show that they processed these transactions—IT access.)
- Master data vs. transactional: This SOD can facilitate various types of fraudulent activity related to fictitious entities (for example, creating a fictitious customer in the customer master data record and processing sales associated with that customer).

Building the SOD matrix

The SOD matrix is a critical component of an effective GRC program. The matrix must be driven by the top-down risk assessment and include any customized functionality. The matrix consists of functions organized in a column and row format showing the business activities which, when combined, produce an SOD conflict.

The matrix should include appropriate considerations for cross-system SOD (i.e., all IT systems used to process transactions in a given business process should be included in the SOD matrix, not just the main ERP system.) Customized functionality is often an overlooked aspect, as standard functions are often included, but custom transactions are not accounted for. After companies include those customizations, they can build out a ruleset to include in an automated GRC solution rather than performing difficult manual reviews.

Compensating and mitigating controls

Once a company develops a list of all SOD conflicts which need to be addressed, it should next identify compensating and, if applicable, mitigating controls. Compensating controls reduce the impact or likelihood of control deficiencies, but do not eliminate it (resulting in a remaining "residual risk" in the environment even if the compensating control operates effectively).

Mitigating controls, on the other hand, completely remove the risk or likelihood of an SOD conflict being exploited in the operating environment. Compensating and mitigating controls can be either automated or manual. Automated controls are more effective, as they are built into the ERP system or deployed through a GRC tool. Even if controls are manual, they should be documented in a CCM/GRC tool.

An important consideration that gets frequently overlooked is continuously monitoring and testing these controls. Companies can have countless controls documented in the system, but without monitoring the continual effectiveness of the control, they likely will weaken over time and may not provide the expected level of protection against risk and fraud.

CCM/GRC tools

CCM/GRC tools are software solutions that provide ways to manage a company's overall IT risk compliance programs, including:

- Internal controls testing and documentation management
- IT policy management
- Dashboard reporting of control findings, with remediation workflows
- Security operations management (such as user access provisioning automation)
- Elevated security access management (often known as "firefighter" access)
- Password change management
- Management of changes made to ERP software
- ERP controls monitoring
- Management of the SOD matrix

There are several CCM/GRC tools on the market, with some aligning better to companies in certain industries, or those with specific technology platforms. Many platforms today can be deployed in a cloud-based software-as-a-service model, whereas others are better suited to a traditional on-premises implementation. Regardless of the solution chosen, governance is key. A tool is only as good as the data that is put into it.

It is critically important to note that implementation of effective ERP SOD and a CCM/GRC tool is never a "set it and forget it" proposition. Maximizing an investment in a CCM/GRC tool, while effectively mitigating SOD risk, requires a well-tuned process. It should periodically reassess organizational business processes and risks, with appropriate changes incorporated into the SOD matrix and CCM/GRC tool on a regular basis.

These changes can be as small as the business wanting an additional function added to the system, or as big as a new business process resulting from a merger or acquisition. Organizations must have a robust policy for reevaluating rules and risks as processes and risk appetites change; otherwise, expensive security redesigns will be necessary or key risks will be overlooked, increasing the potential for fraud.

Why CCM/GRC?

CCM/GRC tools are enablers that implement automated controls and reduce manual processes—and therefore, can reduce opportunities for fraud when utilized appropriately. ERP systems are complex and always changing, and CCM/GRC tools reduce costly compliance efforts, automate user provisioning, and monitor and prevent SOD concerns and sensitive access. GRC tools are also less likely to produce output with errors, such as false positives or false negatives.

When a CCM/GRC tool is implemented correctly, its automated processes create a much more thorough environment for detecting and mitigating fraudulent behavior.

Common CCM/GRC pitfalls

While CCM/GRC tools can offer higher levels of fraud protections, organizations must be wary of potential implementation and maintenance pitfalls. Implementation challenges can include:

- Poor initial configuration
- Poor (or nonexistent) risk assessment
- Lack of ownership
- Customizations (e.g., custom transactions) not considered
- Manual controls not considered in rules (management override)
- Cross-application access not considered (particularly common in environments with a large portfolio of legacy non-ERP applications)

Maintenance issues typically involve:

- No process to periodically update rules
- Poor design of compensating or mitigating controls
- Business changes not accounted for, including:
  - Acquisitions
  - New business lines
  - Technology changes
- Risks or risk assessment never refreshed
- False positives or negatives

Vendor considerations

To overcome these common difficulties, organizations should work with an advisor that understands potential missteps and integration best practices. Many companies believe that a CCM/GRC tool is immediately ready for effective implementation, but that is not the case. A significant amount of attention must be dedicated to ensuring an optimal design, and an experienced risk advisor is often best able to interface with the integration team to balance implementation, operational, strategic and maintenance concerns.

Companies must be careful to evaluate core competencies when considering potential vendors. Vendors specializing in system integration focus on getting the tool up and running, but generally do not have extensive experience around risk and controls. In addition, organizations should consider post-implementation training and whether their vendor will educate users on how to use the tool and how to manage security and define process ownership.

Conclusion

To effectively address and prevent fraud, key business risks and SOD concerns from an ERP standpoint must be identified and mitigated. Companies should perform a comprehensive risk assessment, and customize and validate existing rule sets for completeness.

Achieving effective ERP SOD control is not a "set it and forget it" process; continuous maintenance and improvement are required. However, audit and SOX compliance alone are not enough to cover the risk of fraud exposure due to insufficient ERP controls. Implementing a CCM/GRC tool can enhance SOD controls and support fraud mitigation efforts, but effective governance is key, and the processes and data supporting the tool are far more important than the tool itself.

+1 800 274 3978
www.rsmus.com

This document contains general information, may be based on authorities that are subject to change, and is not a substitute for professional advice or services. This document does not constitute audit, tax, consulting, business, financial, investment, legal or other professional advice, and you should consult a qualified professional advisor before taking any action based on the information herein. RSM US LLP, its affiliates and related entities are not responsible for any loss resulting from or relating to reliance on this document by any person. Internal Revenue Service rules require us to inform you that this communication may be deemed a solicitation to provide tax services. This communication is being sent to individuals who have subscribed to receive it or who we believe would have an interest in the topics discussed.

RSM US LLP is a limited liability partnership and the U.S. member firm of RSM International, a global network of independent audit, tax and consulting firms. The member firms of RSM International collaborate to provide services to global clients, but are separate and distinct legal entities that cannot obligate each other. Each member firm is responsible only for its own acts and omissions, and not those of any other party. Visit rsmus.com/aboutus for more information regarding RSM US LLP and RSM International.