A Risk-based Approach to SoD

Partnering IT and the Business to Meet the Challenges of Global Regulatory Compliance

Michael Adolphson, CISA, CISM, CISSP, CPA, is a senior manager in the advisory practice of Ernst & Young LLP. He can be contacted at *michael.adolphson@ey.com.*

Justin Greis, CISA, CISM, CGEIT, CISSP, CIPP, GIAC/GSEC, ITIL, PMP, is a manager in the advisory practice of Ernst & Young LLP and adjunct professor of information systems at the Kelley School of Business—Indiana University, Bloomington (USA). He can be contacted at *justin.greis@ey.com.*

Segregation of duties (SoD) is a hot topic of conversation among a range of professionals, from compliance managers to executive officers. The outpouring of interest in SoD is due, in part, to the requirements of the Sarbanes-Oxley Act in the US and other similar control-driven regulations worldwide. However, there is another factor at work: the principle that no individual should have excessive system access that enables him/her to execute conflicting end-to-end transactions. If this concept is common sense, why do so many companies struggle with SoD compliance and why does it repeatedly stifle IT, internal audit and finance departments? In large part, the difficulty rests in the complexity and variety of the systems that automate key business processes and the ownership and accountability for controlling those processes.

SoD is a basic internal control that attempts to ensure that no single individual has the authority to execute two or more conflicting sensitive transactions with the potential to impact the financial statements. Without proper guidance and a sound approach, SoD testing, remediation and mitigation may appear daunting or impossible. However, a risk-based methodology can make the effort manageable.

BUSINESS DRIVERS AND GLOBAL REGULATORY COMPLIANCE

Proper SoD is a long-established method of preventing fraud and maintaining checks and balances within a company. However, the recent regulatory focus on public companies has driven businesses to truly understand what access their employees have within their application portfolio. Sarbanes-Oxley not only imposed an unprecedented rigor around controls, it also underscored the importance of an integrated IT and financial controls approach to managing risk within a company.

Across the globe, existing and proposed regulations continue to bring the issue of SoD and controls to the forefront of agendas for auditors and executives alike. These include the European Union's 8th Directive, which is viewed to some degree as Europe's Sarbanes-Oxley equivalent, and Basel II, which addresses the method that financial institutions use to calculate capital adequacy and its alignment with the company's risk profile. The proposed Solvency II sets forth similar regulatory objectives for the European insurance sector. Regardless of country or geographic location, SoD exists as an expectation from investors, clients and capital markets and as a fundamental internal control.

Related developments include Standard and Poor's inclusion of enterprise risk management in its rating considerations and changes related to adopting International Financial Reporting Standards (IFRS). In response, compliance initiatives continually expand and consume corporate resources. As companies rationalize spending and optimize budgets, a pragmatic, balanced approach to internal controls is expected. The Public Company Accounting Oversight Board (PCAOB)'s Auditing Standard No. 5 pushed companies and their auditors to focus more on risk and those control weaknesses that could affect the business and financial statements—a clear message that a risk-based methodology is fundamental to an effective and efficient internal control framework. Yet, even with the direction and trends of global regulations, companies must still confront the challenge of internal bureaucracy since proper SoD cannot be achieved without a partnership between the business and IT.

A RISK-BASED METHODOLOGY

A risk-based methodology, such as the one discussed in this article, focuses on the issues that pose the greatest threat to the business and company's financial statements. Whether the drivers for investing in SoD compliance are fraud prevention, regulatory compliance or a new enterprise resource planning (ERP) system, a company cannot eliminate every potential risk. Rather, the goal is to hone in on the issues that meet predefined thresholds of risk. These are typically determined at the outset of the SoD initiative. Materiality, fraud thresholds or financially significant value limits are examples of thresholds that serve to measure the financial sensitivity of SoD conflicts.

SoD dictates 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. Sensitive transactions drive processes with the potential to impact a company's financial statements. Many companies strive for zero SoD conflicts in their user population, though this expectation is often unattainable, unsustainable and unrealistic, given the number of employees within a typical business function. Separating discrete job responsibilities into task-oriented roles can often result in inefficiencies and unnecessary costs.

Ultimately, it is critical for the company to understand and assess the landscape of current conflicts, minimize them to the extent possible for a given staffing model (via remediation initiatives) and apply financial mitigating controls to the remaining issues. This approach does not yield zero SoD conflicts, but it demonstrates when management evaluates existing conflicts and reduces residual risk to an acceptable level through tested and controlled financial processes. Typically, this solution is palatable to auditors, regulators and financial reporting stakeholders alike, and promotes the awareness of risk beyond a compliance-only exercise.

THE SOD ROAD MAP

Most SoD initiatives consist of five phases: business definition, technical definition, testing, mitigation and remediation, illustrated in **figure 1**.

Business Definition

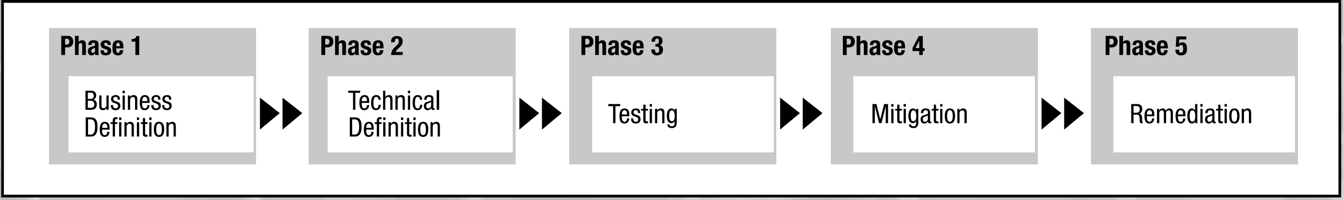
The objective of this phase is to gain an understanding of the scope of sensitive transactions and conflicts that drive the company's key business processes. These are the transactions that pose the greatest fraud risk to the organization should someone possess excessive access. Thresholds are determined based on the risk and monetary impact to the company for each potential SoD conflict pairing.

As this step lays the foundation for everything that follows, proper execution is critical. Many companies fail in this early stage by taking on too many conflict pairings that do not meet the threshold level of risk. For example, a company may be concerned about allowing the same individual to both create a vendor purchase order and modify the customer pricing master file. However, the combination of the two may constitute such a low risk that it does not warrant inclusion in the company's conflict matrix (discussed in the following paragraph). It might be more appropriate to include potential conflicts for a user who could modify the vendor master file, create a vendor purchase order and issue payment to vendors, as this combination represents a higher risk to the company.

The output of the business definition phase is a matrix of potential conflicts, independent of the supporting IT application driving each transaction, but including the corresponding risk statement related to each conflict. The risk statement answers the question, "Why do we care about this transaction pairing?" and demonstrates what could go wrong if an individual had enough access to create a conflict. In the example above, the risk statement might say, "A user could create a fictitious vendor or change vendor master data, initiate purchases to this vendor, and issue payment to this vendor." In this case, the vendor might be the fraudulent employee with an excessive and inappropriate level of access in the system.

Generally, the matrix and corresponding risk statements differ among companies, industries, business models and even locations within the same company, depending on what processes are financially significant. It is not uncommon for

Figure 1—The SoD Road Map



a large global company to have more than one matrix due to differences in the business processes by location or business unit. For example, a company may have a manufacturing business unit with a large amount of inventory, requiring an SoD matrix that focuses on specific inventory transactions. It may also have a service-based business unit, necessitating a focus on project accounting and requiring a different SoD matrix. Though knowledge of similar businesses and industries can help to establish the conflict matrix, each business unit must perform a customized analysis of its conflicting transactions to capture the real risk for that particular business model.

Technical Definition

The technical definition uses the completed conflict matrix as a tool to help answer the question, "Which applications are able to execute the defined sensitive transactions and how are they executed in the system?" The company or business unit must map each sensitive transaction to its associated access rights in the application that enables that transaction. This critical step feeds the data analysis to yield the testing results. While this mapping task may appear to be simple, this step is often where many companies encounter problems due to lack of understanding of the potential ways a transaction could be executed in a particular application.

Testing

The testing phase draws on data from the business definition and technical definition phases to produce an analysis of users with SoD conflicts. This report highlights the SoD conflicts in a number of ways, such as by user and by role/group, and shows the extent of the conflicts among the company's user population. This analysis, in combination with the business and technical definitions, typically serves as the compliance testing package disclosed to audit parties and regulators.

Mitigation

The mitigation phase can be completed concurrently with remediation, or, depending on one's objectives and compliance time frame, mitigation can be performed last, once conflicts have been reduced to their absolute minimum. Mitigation examines each of the identified SoD conflicts and asks, "Which effective financial controls (generally evidenced via testing documentation as part of a Sarbanes-Oxley initiative) can be cited to demonstrate that the residual risk of a particular SoD conflict does not pose a financially significant threat to the business?" In other words, can the company cite any existing controls that will detect the unauthorized or fraudulent activity? Mitigation has several critical success factors. Many companies choose to mitigate every potential conflict to establish a safety net of control should a conflict arise. This is a sound and practical strategy for companies looking to control unforeseen or unpredictable risk.

Remediation

The goal of this phase is the permanent correction of SoD conflicts. Remediation techniques include role redesign, role cleanup, user appropriateness review and SoD tool implementation. A combination of people, process and technology changes help sustain compliance. There is no prescribed road map or universal method for remediating conflicts. Each scenario is unique, depending on the degree of complexity and extent of the conflicts in a given environment.

CONCLUSION

SoD remains an integral part of a company's internal controls. While the appropriate level of effort and emphasis needs to be placed on SoD compliance, companies must also strive for simplicity and precision in the execution of their controls. SoD presents a unique challenge to control compliance as it requires close alignment of business and IT stakeholders to identify, assess, reduce and monitor the risk of fraud or material misstatement.

Spending money on applications and tools intended to fix deficient processes and expecting them to improve over time is not a sustainable compliance or IT strategy. Company leaders must take a step back and ask what the enterprise is trying to accomplish through SoD. A well-designed, risk-based SoD initiative can not only enable global compliance, it can also demonstrate value by enhancing controls while improving, streamlining and efficiently redesigning key business and IT processes.

AUTHORS' NOTE

The views expressed herein are those of the authors and do not necessarily reflect the views of Ernst & Young LLP.