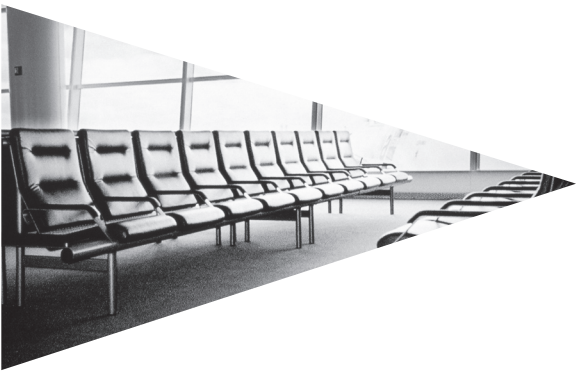
October 2008

Executive summary



A risk-based approach to segregation of duties

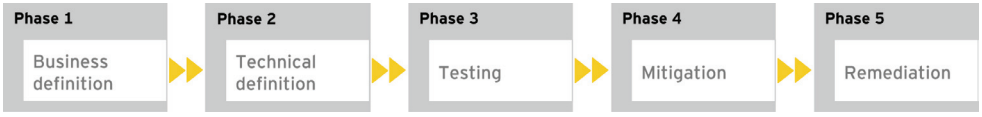
Segregation of Duties (SoD) remains elusive for many organizations even though its operating principle is quite simple: no individual should have excessive system access that allows them to commit fraud or materially impact the financial statements. The challenge lies primarily in the complexity of the interconnected systems and processes that exist in many modern enterprises. Spurred by Sarbanes-Oxley and similar control-related regulations worldwide, companies have never had a greater incentive to establish rigorous SoD policies and procedures.

By focusing on the transactions that pose the greatest risk to the business, a company can quickly gain control over the underlying access issues and determine — at a level that satisfies management, regulators and audit parties — that appropriate steps are being taken to remediate and mitigate the root causes of the issues.

Well before computers played a vital role in companies' automated processes, SoD existed as a basic internal control that attempted to ensure no single individual had the authority to execute two or more conflicting sensitive transactions. Technology and integrated systems introduced a new level of complexity by creating multiple avenues for transaction processing. While technology brought flexibility, efficiency and agility into business processes, its use also generated a distinct form of risk and the potential for fraud and material misstatement.

Most SoD initiatives consist of five phases: (1) business definition, (2) technical definition, (3) testing, (4) mitigation and (5) remediation. The goal in business definition is to understand the risk and scope of sensitive transactions to be analyzed. The output is a matrix of potential conflicts that articulates what could go wrong should someone have enough access to create a conflict. During the technical definition phase, the company or business unit maps each sensitive transaction to its associated application and access rights. Access rights are the lowest possible level of security available in an application. The results of the these first two phases form the basis of the testing that 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 organization's user population.

The SoD roadmap



Michael Adolphson, + 1 312 879 3769, michael.adolphson@ey.com, is a senior manager in the IT Advisory practice of Ernst & Young LLP.

Justin Greis, + 1 312 879 2266, justin.greis@ey.com, is a manager in the IT Advisory practice of Ernst & Young LLP.

They are based in Chicago.

ERNST & YOUNG
Quality In Everything We Do

Armed with the knowledge from the first three phases, the enterprise is prepared to identify existing internal financial controls that will detect and prevent — and therefore mitigate — the consequences of unauthorized activity. Many companies choose to mitigate every potential conflict in order to build a safety net of control should a conflict arise. However, ongoing utilization of mitigating controls without remediation of the root-cause system access issues is not sustainable for most organizations. Remediation techniques include role redesign, role cleanup, user appropriateness review and SoD tool implementation. Techniques such as these seek to build tangible capabilities for the company and address the heart of the underlying risk: excessive user access to conflicting sensitive transactions.

Every scenario is unique depending on the degree of complexity and extent of the conflicts in a given environment. A well-designed, risk-based SoD initiative can not only enable compliance, but also demonstrate real business value by enhancing controls while improving, streamlining and efficiently redesigning key business and IT processes.

Ernst & Young

Assurance | Tax | Transactions | Advisory

About Ernst & Young
Ernst & Young is a global leader in assurance, tax, transaction and advisory services. Worldwide, our 135,000 people are united by our shared values and an unwavering commitment to quality. We make a difference by helping our people, our clients and our wider communities achieve their potential.

About Ernst & Young's Technology and Security Risk Services
Information technology is one of the key enablers for modern organizations to compete. Effective information technology risk management helps you to improve the competitive advantage of your information technology operations, to make these operations more cost efficient and to manage down the risks related to running your systems. Our 6,000 information technology risk professionals work with you to develop an integrated, holistic approach to your information technology risk or to deal with a specific risk and security issue – wherever you are in the world. And we work to give you the benefit of our broad sector experience, our deep subject matter knowledge and the latest insights from our work worldwide. It's how Ernst & Young makes a difference.

www.ey.com