

A White Paper on

**Segregation of Duties**  
And how Avaap's Security Dashboard  
helps monitor Lawson access

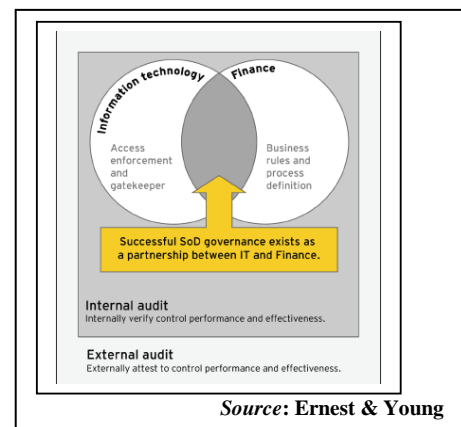


## Executive Summary

SoD is a control concept that essentially means the “fox should be explicitly prevented from watching the henhouse”. A traditional application of this control is requiring the audit department to report outside the chain of people it is auditing to reduce conflict of interest. In the context of ERP tool, it is expressed in controls over finance activities typically preventing a single person from having the control to both create and pay vendor.

Most organizations have not effectively addressed SoD conflicts and are saddled with thousands of conflicts throughout multiple ERP instantiations. These conflicts can be difficult to identify, and the identification process requires accounting knowledge and institutional knowledge of the specific ERP instance. Poorly conceived roles and ad hoc role management increase the

complexity making it difficult to identify user accounts with excessive levels of access. Manual analysis process fails to identify all such role conflicts. Static analytical tools present both preventive and reactive technique for monitoring and compliance reporting. This white paper introduces the concept of Segregation of Duties (SoD), highlights the challenges to managing SoD and discusses Avaap’s Security Dashboard solution as a useful and cost-effective tool for identifying conflicts.



*Source: Ernest & Young*

## **Introduction**

Segregation of Duties (SOD) has much greater scrutiny with the process controls requirements mandated by Section 404 of the Sarbanes Oxley Act (SOX). Segregation of duties should include the assurance that no one individual has the physical and system access to control all phases of a business process or transaction: from authorization to custody to record keeping. In other words, no individual should have excessive system access that enables them to execute conflicting end-to-end transactions.

When conflicts exist in segregation of duties, organizations can be exposed to significant risks. Auditors are looking for conflicts in segregation of duties in which one individual has access to responsibilities which are inherently in conflict with one another, such as purchasing and accounts payable, purchasing and receiving, general ledger and supply management, etc. The conflicts can be caused by innocent and unintentional errors or by intentional and criminal fraud. A good business practice would argue that supplier master control should be segregated from all supply chain, procurement and payables responsibilities. Entering a supplier, which is a key function, should not be held by anyone who has the ability to enter invoices or enter purchase orders.

Interestingly, the need to handle SoD conflicts seems to have dawned quite suddenly upon the industry. The annual Hype Cycle report for Identity and Access Management published by Gartner in 2005 did not mention SoD at all whereas the 2006 edition placed "SoD for ERP" as being already past the peak. By 2007 "SoD for ERP" was in the 'Trough of Disillusionment' and through 2008 and 2009 it matured, 'Climbing the Slope' in Gartner terms.

## **The Segregation of Duties Challenge**

Many organizations struggle with implementing a simple SoD as they quickly determine its consequences. One of the biggest challenges is the ability to override the given controls based on positional authority. For instance, SoD often does not address conflicts that emerge when employees with conflicting functions report to the same supervisor or manager. A well-designed segregation of duties matrix is generally expected to greatly reduce the chances of unilateral errors or fraud, as these require collusion between or among multiple employees in order for errors to occur without detection. One of the overbearing considerations while designing effective segregation of duties relates to hierarchical approvals. An example of hierarchical approvals is the increasing dollar values of purchase order approval as they go up

the hierarchy. Also, the traditional approach to developing and monitoring SoD often leaves out the possibility that the process controls can be overridden at some level of the organization. Further complicating the ability to maintain segregation of duties and provide viable checks and balances, consider the same reporting relationship in a global organization in which each functional area is located in different time zones or even different continents, with users speaking different languages.

Various surveys have shown that most fraud is committed at executive levels of organizations. This is not to minimize the impact of fraud at lower levels, which SoD will help to prevent. Due to the complexities in the maintenance and support of ERP applications, many IT departments have virtually unlimited access to the "production environment" as System Administrators or as Super Users. Granting access to a production system to such Super Users adds a level of risk as they may override the controls during system support. Unlike in mainframe environments, technology limitations in the database make it impossible from a performance perspective to provide a complete audit trail on a user, especially in case of extreme volume in some transactional tables such as where payables invoices or purchase orders are stored.

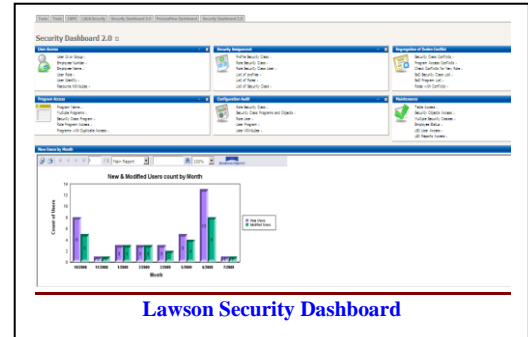
The role of the System Administrator is another area of significant risk. The System Administrator role grants access to business functions. In many companies, the System Administrator is the final gatekeeper to prevent a user from getting access to two or more functions that could give that user the ability to violate SoD. Because of this role, they inevitably become familiar with how a user is able to violate good controls. With this knowledge and the System Administrator role they have the ability to violate SoD and internal controls. Write access to the database adds even further risk and should be considered as well in the design of SoD controls.

Finally, organizations are challenged by complex legislations. The Sarbanes-Oxley Act and its European equivalents (IAS/IFS and Basel2) require rigid and diligent control over all finance-related transactions (e.g., sales orders, purchase orders, warehouse deliveries). Staying in compliance requires a variety of tools and technologies. The bottom line - no single ERP, system control tool or ingenious methodology can ensure foolproof SoD. It requires a combination of these to arrive at an optimum design. Each business unit must perform a customized analysis of its conflicting transactions in order to capture the real risk for that particular business model.

## A Quick Tour of How Avaap's Security Dashboard monitors Segregation of Duties

Lawson utilizes Role Based Access Control models for access control. With this model, business rules are cast into roles leading to authorization decisions that either say "yes, you may because it's in your role" or "no, you may not because it is not in your role".

These business rules are encapsulated within 'Security Classes'. Thus, a tool that compares roles or business rules and picks out potential conflicts goes a long way towards optimizing SoD design and fulfilling audit requirements.



Organizations may have to monitor the conflicts with the aid of an external mechanism like excel spreadsheet or homegrown tools. These would still be up for scrutiny during statutory audits. Without a sound approach, SoD validation, remediation, and mitigation may appear daunting. Avaap has plugged this gap in a very user-friendly way as part of their Security Dashboard. The Segregation of Duties module of reports provides simple, easy-to-use functionality for monitoring SoD.

Organizations can identify and configuring known conflicts from security classes or programs on Avaap's delivered SoD forms. Auditors and administrators can then run Security Dashboard reports against these pre defined SoD rules and quickly identify possible conflicts.

Lawson SOD Security Class Conflicts List (ZS12.1)

Security Class	Description
APCycleProcessing	AP Cycle Processing
APSetup	AP Set up

Avaap Screen for defining Security Class SoD rules

System Administrators or super users often have access to the production environment where they can alter or override control. Lawson Security records these security violations attempts, as well as users who perform changes to Lawson Security settings. The Avaap Security Dashboard reports can display these attempted violations and security setup changes.

By focusing on transactions that pose the greatest risk to the business the Security Dashboard can help a company quickly gain control over the underlying access issues. Management can then be assured (at a level that satisfies management, regulators and

audit parties) that the appropriate actions are being taken to remediate and mitigate the root causes of the issues.

## **Conclusion**

SoD is not a project, but a process. It needs to continue into the future. The longer term undertaking is much easier if tasks are performed early on. Thus an investment in sound practices and processes today will inevitably lead to savings down the road.

Business process improvement challenges require practical, easy-to-use and ready-to-implement solutions. The ultimate purpose is to translate business strategies into operational actions that can secure profitable bottom line benefits to the company's shareholders. Avaap Security Dashboard is a strategic solution that takes controls monitoring to the next level by combining business roles and rules essaying with conflict analysis and audit reporting. It offers the advanced tools necessary to help organizations meet their increasingly challenging SoD needs, including their ability to provide detective controls for best practices in corporate governance, compliance and risk management.

It must be understood that the Security Dashboard is only one of several tools to identify conflicts. It is intended to highlight potentially conflicting duties, but is not intended to be the only method of identifying all such conflicting duties. Additional reporting and review processes or spot checks may be included to ensure identification of fraud. Physical, mechanical, and electronic controls go hand in hand in safeguarding the business interest. There should be sufficient procedures of who requisitions the material from stores; there should be proper cameras at various locations to keep a track of people coming in going out; assets should be properly numbered and stock taking should take place at the end of every year and 'Segregation of Duties' guidelines and internal control check list should be strictly enforced.

After all, trust is not an issue; verifying business transaction is.

## **About Avaap**

Avaap Inc. is one of the fastest growing Lawson Professional Services company. Avaap has been set up with the clear perception of creating a world-class software development enterprise to deliver innovative, high quality, cost effective solutions and services in enterprise systems domain. Avaap enjoys very high customer retention due to their outcome driven methodology and was one of the first companies to offer a Fixed-Price offering for upgrading clients to Lawson applications 9.0.

Avaap Inc. seeks to leverage its subject matter expertise in Lawson Technologies to provide innovative and Outcome Based services in a very cost effective manner. Avaap offers best in class consulting services that focus on an outcome based approach by leveraging key metrics that can track the success/failure of a given project at identified milestones

**Call [732-321-4326](tel:732-321-4326) or mail [info@avaap.com](mailto:info@avaap.com) to arrange for a free product demonstration of Avaap's Security Dashboard**

## **Reference**

"Hierarchical Segregation of Duties" by Anthony Tarantino, Cutter IT Journal, Volume 7, Number 22, December 2004.  
"Market scope for Segregation of Duties Control within ERP, 2007", Gartner  
"Risk based Approach to Segregation of Duties", Ernest & Young  
"Enforcing Segregation of Duties", White Paper by Axiomatics