



Defect-Free  
Financial  
Processes

## **Segregation of Duties in the Real World**

Risk-Based SoD Management  
with Continuous Monitoring  
Lowers Compliance Costs

Like controls documentation and access provisioning in previous years, segregation of duties management is part of this year's initiative for auditors and their review of your internal controls. Unfortunately, this can escalate the already excessive costs of Sarbanes-Oxley compliance if companies continue to manage and test their internal controls like they have in the first years under Section 404 of the Enron-inspired law.

With a bottom-up approach to implementing and testing controls, companies spent millions to document and validate low-level process controls without consideration of financial risk. These largely manual efforts led to rather tedious work that consumed thousands of man hours and produced minimal benefit.

To extend this bottom-up approach for segregation of duties controls, companies are forced to identify all users of corporate financial systems that can potentially violate SoDs and then reconfigure – or redeploy – the ERP systems to eliminate the SoD weaknesses. However, most financial executives realize that all segregation of duties weaknesses cannot be completely eliminated without re-engineering financial processes or hiring dozens of new employees to properly separate functions without overlapping responsibilities.

Compliance costs then shift from mundane controls testing and documentation to complex IT projects and permanent additions to overhead costs. In many cases, the cost to eliminate a SoD weakness far exceeds its financial risk.

Segregation of duties in the real world demands top-down management that eliminates financial risk without adding overhead costs or extinguishing ERP-fueled efficiency gains of the last decade. Fortunately, auditors and government regulators are moving beyond simple checklists of mandates to advocate a risk-based approach to SOX compliance and internal controls. This is great news for finance executives and compliance managers who can lead their companies to reduce compliance costs while accomplishing the ultimate goal of SOX – financial integrity.

This white paper highlights the challenges to managing segregation of duties, builds a case for risk-based SoD management, and discusses technology solutions for continuous monitoring that deliver affordable and effective SOX compliance.

*It's almost always cheaper to implement a top-down approach, and more effective at controlling risks.*

**– Compliance Week, June 2006**

### **The SoD & Compliance Challenge**

Sarbanes-Oxley certainly did not introduce the concepts or principles of segregation of duties. Separating financial functions across individuals has always been good business practice to reduce the risk of fraud and check the accuracy of financial transactions. However, the challenges of managing and maintaining proper segregation of duties is now a complicated task that involves thousands of ERP users, heterogeneous financial systems, and an over-reliance on manual controls that mitigate weak ERP controls.

For companies who adopt a bottom-up approach for segregation of duties management, the key tenet – and overwhelming obstacle – is that every segregation of duties conflict can and should be prevented through tight configuration of financial systems for stringent controls. To accomplish this, these companies must rely on compliance teams drawn from IT, finance, and audit to:

- Analyze all authorized users of financial systems
- Identify access rights and roles that can potentially violate segregation of duties
- Reconfigure ERP and financial systems with new user roles.

### **Financial System Users & SoD Conflicts**

Bottom-up enforcement of segregation of duties starts with analyzing the access rights and responsibilities for all financial system users – from

accounts payable clerks to the CFO. Manual analysis can be terribly consuming as each user's access rights are compared against a matrix that shows 100s of potential SoD control conflicts for each business process.

While ERP configuration tools can assist with analysis, the results can be quite overwhelming. A Fortune 500 company with 5,000 SAP users can expect to find upwards of 20,000 individual SoD control conflicts where an ERP user has two discreet privileges that allow for a potential SoD violation. The bottom-up approach then mandates that each of these 20,000 SoD conflicts be resolved by defining new roles, eliminating management roles with override privileges, and adapting financial processes to meet SoD demands.

*A bottom-up approach treats every risk equally, and applies the same level of detailed examination to the processes required to control those risks. This results in the needless review of many areas containing little, if any, risk.*

**– Harvey Pitt  
Compliance Week Columnist &  
Former Chairman of the SEC,  
June 2006**

### **Unavoidable & Low-Risk SoD Conflicts**

However, this intensive, manual effort still does not effectively address all segregation of duties weaknesses. Most companies face environments where financial processes cannot be completed without allowing for some form of SoD conflicts within user access rights. For example, a remote office may not have enough people in finance to stringently divide ERP functional responsibilities. Other processes demand that at least some managers retain “super user” privileges within the financial systems. And still some SoD conflicts present such a low risk that the cost to reconfigure the ERP system to correct the SoD conflict far exceeds the risk.

In these cases, companies must implement manual mitigating controls that require personal review and sign off on every transaction to inspect for potential SoD violations. Because manual controls are less reliable than automated controls, they must be tested more often and more intensely to ensure effectiveness. This in turn drives increased compliance costs.

### **Segregation of Duties Reality Check**

Most financial executives recognize the flaws in this bottom-up approach to managing segregation of duties. According to the *2006 Oversight Systems Financial Executive Report on SOX*, 90 percent of financial executives say that SoD conflicts cannot be eliminated through ERP configuration. When asked to name the major challenges faced in maintaining SoDs, 70 percent said keeping up-to-date with changes to roles and access rights, such as promotions, transfers and terminations, among system users. Other major SoD challenges include ensuring proper segregation of duties in remote offices and in organizations with small financial staffs (49 percent), and monitoring activities of “super users” (47 percent).

All segregation of duties issues cannot be effectively handled with preventive access and authorization controls. In the real world, financial systems must allow financial managers to effectively and efficiently do their jobs. A bottom-up approach to managing segregation of duties ignores financial risk and drives SoD controls to every ERP user without regard to process disruptions and escalating costs.

To roll back compliance costs, companies should evaluate a risk-based approach to compliance that effectively addresses all segregation of duties.

### **Risk-Based Segregation of Duties**

As the Public Company Accounting Oversight Board pushes auditors to abandon their initial bottom-up approach to controls testing, companies should follow suit with top-down, risk-based controls – including those for segregation of duties.

The challenge for finance executives and compliance managers is to implement controls that meet their auditor's expectations.

The PCAOB's May 2005 published comments on Audit Standard No. 2 provide guidance for auditors to adapt their SOX 404 audits to be more in-line with the law's intent – financial integrity.

*A top-down approach prevents the auditor from spending unnecessary time and effort understanding a process or control that does not affect the likelihood that the company's financial statements could be materially misstated.*

**– PCAOB Auditing Internal Control over Financial Reporting, May 2005**

The key for finance executives and compliance managers to meet their auditor's expectations with risk-based, top-down segregation of duties is to recognize the difference between "theoretical" risk of what could happen and "relevant" risk to financial reporting. Instead of focusing on correcting the potential 20,000 individual SoD conflicts, a risk-based approach to segregation of duties:

- Prioritizes SoD conflicts based on risk & actual violations
- Designs and implements preventive controls that address relevant risk where possible
- Implements automated mitigating controls for unavoidable and low-risk SoD conflicts.

### *Prioritizing SoD Weaknesses*

Rather than approaching every SoD conflict with equal importance, risk-based segregation considers each conflict in the context of its effect on financial integrity and the likelihood of actual violations. To appropriately determine risk and prioritization, companies should analyze each individual SoD conflict for:

- Who actually violated the SoD conflict
- How often has the conflict been violated

- What's the aggregate dollar-value of violations to this SoD

This historical analysis – along with top-down view of how each control affects financial integrity – provides the risk-based prioritization of SoD conflicts. Your compliance team can then build a work plan that focuses on the highest priorities to address the greatest risks to financial integrity and ensure effective controls for SOX compliance.

### *Automated Mitigating Controls*

Instead of consuming thousands of work hours to correct every individual SoD conflict within your ERP system, a risk-based approach to segregation of duties recognizes that some conflicts cannot be eliminated without massive re-engineering of the financial process. And other SoD conflicts represent very low risk. In short, some ERP control deficiencies cannot be corrected in the ERP system and other ERP control deficiencies don't present a big enough risk to justify a redeployment of the ERP system.

To address these SoD conflicts, companies have traditionally relied upon manual controls that review transaction logs on a monthly or quarterly basis. While these manual controls introduce extra work in business processes to log activities and review transactions, auditors have viewed these manual controls as not as reliable because they rely upon manual intervention. And for this reason, auditors spend more time testing these manual controls, which then increases the cost of compliance.

But mitigating controls no longer have to be manual. In fact, technology solutions can provide automated mitigating controls that eliminate management's burden to carry out manual controls and satisfy your auditor's demands for effective SoD management.

Real-time monitoring of financial processes provides fully automated mitigating controls that effectively manage segregation of duties for both low-risk SoDs and privileged ERP users by:

- Logging all ERP activities into a secure audit log

- Analyzing every new transaction against all previous transactions
- Reporting all transaction-level SoD violations
- Providing a case management framework for resolving every violation.

### Challenges to Risk-Based SoDs

Risk-based management of segregation of duties greatly depends upon automating your internal controls and managing SoD risk across all the entirety of financial processes. As mentioned above, auditors place greater value on automated controls that don't rely on human intervention. Thus, continuous monitoring of financial processes for SoD management must be fully automated and real time.

Many monitoring solutions require IT managers to periodically run reports against their ERP systems to identify potential SoD violations – either in the access rights or historical transactions. But this manual process of running reports and reviewing transaction logs remains a manual control that auditors regard as less reliable and requires extensive testing.

Second, financial executives and compliance managers should recognize that managing segregation of duties is not an ERP issue; it's a process problem. Segregation of duties must be managed across financial processes and not just individually within each financial system. It's not enough to have locked-down user access rights in SAP if customer master files are managed in Siebel. In this case, proper SoDs must be managed across the entire order-to-cash process and across every financial system that supports the process.

### The Oversight Solution for Risk-Based Segregation of Duties Management

Oversight Systems enables risk-based management of segregation of duties by combining user access rights testing with its patented real-time transaction inspection. Preventive controls fuse with automated mitigating controls to deliver

complete SoD management that reduces the costs and burden of Sarbanes-Oxley compliance.

Until Oversight, companies had to choose between controls software that either tested a single ERP system for SoD conflicts or analyzed historical transactions for control violations. However, the Oversight solution for risk-based SoD management builds upon each of these first generation technologies to:

- Identify SoD conflicts across heterogeneous financial systems
- Analyze all historical transactions to determine if SoDs were ever violated
- Prioritize corrective actions based on actual risk of where SoD violations have occurred
- Automate mitigating controls for remaining SoD conflicts
- Prove SoD compliance with automated documentation and case management.

### Identify SoD Conflicts

Because financial processes rarely operated in a single ERP system, Oversight integrates with all major ERP systems – SAP, Oracle, PeopleSoft, JD Edwards – as well as the many “feeder” systems, such as MFG Pro, Infinium and legacy applications. Oversight analyzes user access rights across all platforms in relationship with every other financial system to identify segregation of duties conflicts where a single user has the potential to violate SoD principles within a single financial system or across multiple systems.

Platform-specific solutions that focus on a single ERP system, such as SAP or Oracle, serve to lock down those systems but ignore the feeder systems. The Oversight solution manages segregation of duties through out the business process and every financial system involved in that process.

### Measure Risk & Prioritize Remediation

Platform-specific SoD scanning tools typically identify thousands of control conflicts for a large enterprise. However, financial process managers and compliance officers are then left to decide which of these 1,000-plus violations must be fixed first. As auditors implement a new risk-based

approach to testing control effectiveness, enterprises must be able to measure the risk associated with each SoD conflict and prioritize corrective actions accordingly.

For each identified SoD conflict within user access rights, Oversight analyzes historical transactions to determine if a user ever carried out a transaction that created an actual SoD violation. Oversight quantifies the risk associated with each SoD conflict, so that financial process managers and compliance officers can then prioritize SoD conflicts for final resolution.

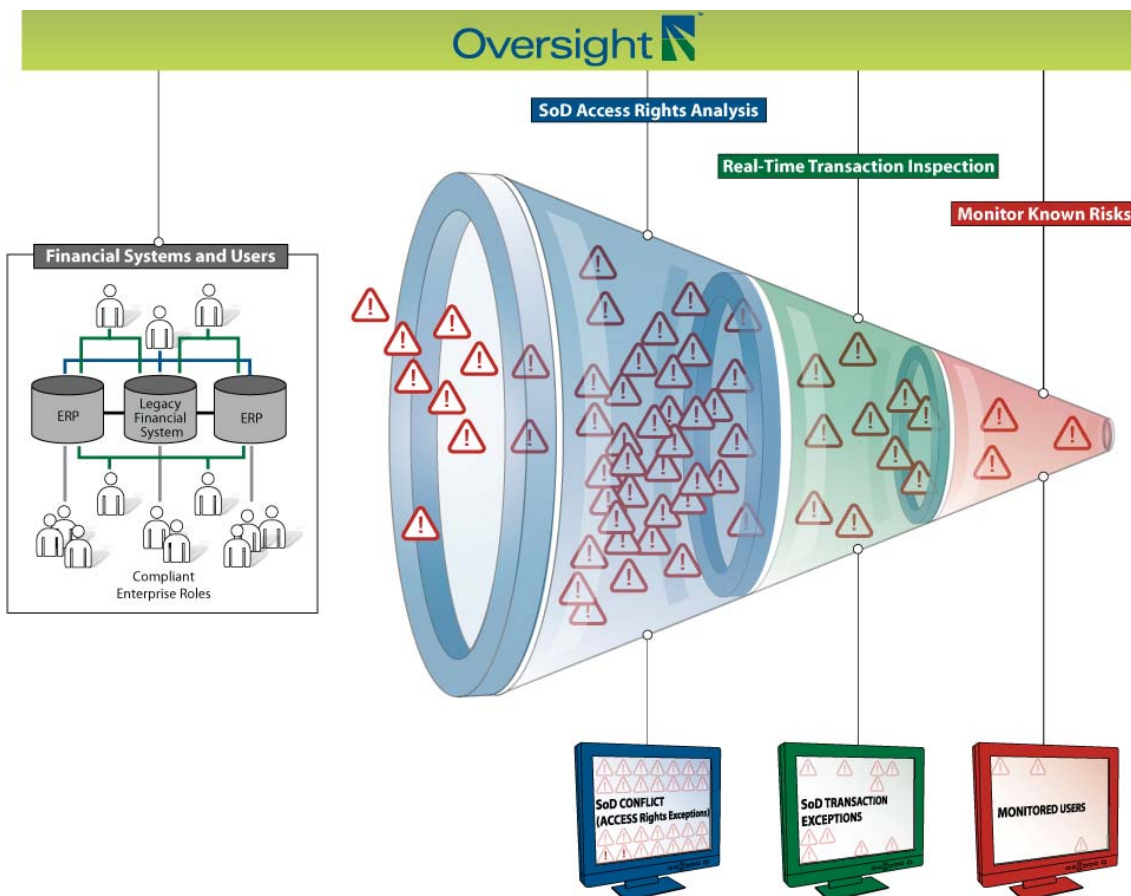
### Automated Mitigating Controls

Because financial processes don't operate in a vacuum, financial process managers and compliance officers recognize that all SoD conflicts cannot – or should not – be eliminated. Sometimes it's just not feasible to hire enough bodies just to separate roles in a financial process. For this

reason, enterprises have typically assigned manual, mitigating controls that require a financial manager to download and inspect a report from the ERP system. These manual controls rely on historical analysis and unwavering diligence from those reviewing the report.

Oversight Systems applies its patented software for real-time transaction inspection to provide an automated mitigating control. For every SoD conflict that cannot be eliminated, Oversight assigns an *Integrity Check* that tests every transaction for SoD violations. Instead of reviewing a monthly report, financial managers receive an alert to the SoD violation the minute the transaction is processed.

Oversight's automated mitigating controls also provide an effective solution for low-risk SoD conflicts within your ERP systems. For segregation of duties conflicts that are rarely if ever violated,



Oversight monitors every transaction for actual SoD violations. Rather than redeploying or reconfiguring the ERP system to eliminate SoD conflicts with insignificant risk, real-time transaction inspection provides an automated mitigating control that effectively manages financial risk.

### *Prove Effective Segregation of Duties*

For compliance with Section 404 of Sarbanes-Oxley, it's not enough to have effective controls. Companies must prove the effectiveness of their controls. The Oversight solution for risk-based segregation of duties management provides this proof by:

- Maintaining a log of all financial transactions
- Providing a case management framework for resolving all reported exceptions
- Reporting on the resolution and status of all exceptions.

For its detailed inspection and analysis, Oversight logs all transactions in its *Secure Audit Journal* to compare every new transaction to historical transactions. Finance executives, compliance managers, and auditors can also access and run reports against this audit data warehouse for a complete log of financial transactions.

After reporting an SoD exception, Oversight correlates all related exceptions and aggregates all relevant information into a case management framework. Oversight's case management provides compliance and finance managers with the information they need to make informed decisions and document their actions and resolution.

Auditors and financial executives can then review the status of all reported exceptions, drill down into specifics details of a single exception, and view exception types across users, sub-processes, and financial systems.

## **CONCLUSION**

As auditors heighten their focus on segregation of duties management, financial executives and compliance managers should avoid repeating the pains and costs of a bottom-up approach to internal controls. Instead of devoting thousands of man hours to reconfigure or deploy financial systems, companies should evaluate and implement risk-based management of segregation of duties.

Rather than spending millions of dollars to address low-risk control weaknesses, risk-based SoD management guides your company to ensure financial integrity and meet your auditor's demands without accelerating compliance costs. Continuous monitoring solutions from Oversight Systems drive risk-based SoD management by automating the analysis of user access rights across all financial systems, prioritizing SoD conflicts by actual risk, and automating mitigating controls for unavoidable and low-risk conflicts.

“With Oversight, I have a system that detects what's going on independent of the accounting or database system. I'm in a much better position if someone in my technology group is manipulating the data.”

*Mike Sullivan*  
*Director of Accounting Services*  
*American Electric Power*

“Oversight helps cut auditing expenses.”  
*Baseline Magazine*

“Oversight works across the financial systems to identify segregation of duties conflicts and prioritizes these conflicts based on actual risk. For the conflicts that can't be eliminated, Oversight's real-time transaction inspection serves as an automated mitigating control to provide alerts when an SoD conflict is actually violated. Instead of having to hunt down and correct every SoD conflict, Oversight enables a risk-based approach to control compliance that allows efficient, defect-free financial processes.”

*Mark Van Holsbeck*  
*Director of Information Security*  
*Averv Dennison*

“Oversight software within minutes found the duplicate payments that nearly paid for the Oversight software immediately. That's a textbook definition of a quick ROI.”

*William McNeill*  
*AMR Research*

“Oversight's benefits of early detection and quick resolution should pay for this system easily.”

*John Hagerty*  
*Vice President*  
*AMR Research*

“Controls automation and monitoring improves reliability of controls and potentially reduces the cost of compliance by reducing the labor component of compliance activities.”

*French Caldwell*  
*Vice President of Research*  
*Gartner*

## About Oversight

Errors in day-to-day financial transactions consistently result in adjustments, reversals and rework. Oversight Systems drives defect-free financial processes to eliminate these extra costly efforts. Increasing the quality of financial operations leads to accelerated, more accurate closes and validates policy compliance. Our software inspects each step of every financial transaction in real time for errors and control violations, so companies can address these issues when they are less complex and less costly to correct.

For more information, visit  
[www.oversightsystems.com](http://www.oversightsystems.com).

Oversight 

[oversightsystems.com](http://oversightsystems.com)  
404.920.2030