ControlPanel GRC

SYMMETRY™

CONTROLPANEL[GRC] ALWAYS AUDIT READY™ SERIES:

Segregation of Duties (SoD)

Five signs that a new SoD compliance strategy needs to be implemented

SoD compliance in 2012 is not the same as it was in 2002

SoD strategies or solutions that worked ten years ago have become unmanageable for many organizations because "first generation" GRC tools and manual processes have not able to keep up with auditor demands in 2012.

Many enterprises must live with known SoD violations given their size or worker mix (for example, an employee in the field office may have to create purchase orders and receive goods). Auditors require that mitigating controls be implemented and reported upon to demonstrate that a risk has been "double checked" to help ensure fraud has not occurred (Who was notified that Alice created a PO and received goods from the same vendor? Was there a documented review?).

Increasingly, external auditors are broadening their purview and depth of inquiry into demonstrable SoD controls. Audits are moving from periodic samplings to a demand for all-the-time, no-exception execution. More comprehensive audits, outdated (or outgrown) software tools, and limited internal resources have created environments where many organizations realize their internal controls aren't at the level they need to be.

ControlPanel GRC

SYMMETRY™

Background on SoD

SoD compliance is one of the key internal controls safeguards in the decade-old Sarbanes-Oxley (SOX) legislation. To comply with SoD requirements, companies have looked to their IT system of record, typically an ERP solution, to track activity. Why? A high proportion of SOX internal control issues can arise in enterprise's core ERP systems. Role-based access controls, commonly managed by ERP administrators in IT, are used to mitigate SoD issues. However, modern ERP systems are complex and managing access to successfully manage potential SoD issues can be tricky. Reporting on SoD conditions for audit can be difficult and tedious. As a result, most companies comply with SoD requirements via specialized governance, risk, and compliance (GRC) solutions or tedious manual processes – like spreadsheets and reports from various off-the-shelf software tools.

Five signs that a new SoD compliance strategy needs to be implemented

When installing compliance automation solutions, we've seen five key reasons, or triggers, that mandate a change in how SoD compliance is tracked and reported.

1. Manual controls are inadequate or too time-consuming
2. Change in audit firms – "new sheriff is in town" mandates changes
3. First generation GRC solutions expensive, often never fully implemented and cumbersome
4. A negative audit finding necessitates a change
5. A "near miss" or bona fide incident occurs, resulting in a need to change

1. Manual Controls are inadequate or too time-consuming

No doubt about it - manual preparation of SoD compliance reporting is tedious and time consuming. Staff that could otherwise be working on valueadd initiatives often spend weeks if not months on compiling reports and responding subsequent inquiries. Since auditors tend to deem manual reports more suspect than automated reporting, responding to more vigorous scrutiny also adds time.

Especially in these post-recessionary times, internal IT organizations have been paired to minimum. With lean IT staffing, the workload of performing manual effective SoD analysis among the daily flood of user add/change/ delete requests can become

ControlPanel GRC

SYMMETRY™

untenable. Time spent on operational, non-value add tasks like compliance reporting rob time available for initiatives. The time spent preparing audit reports "doesn't sell us more paint" as one consumer products CFO lamented. There is an opportunity cost as well as the actual costs.

IT staff bear the brunt of manual preparation of SoD compliance reporting, but also business unit role owners also need to participate, again distracting them from their primary duties. CIOs and CFOs can face unpleasant questions from their Board of Directors if audit findings are not satisfactory.

Other than the amount of time and staff needed to prepare manual SoD reports, we have also found that there are several compliance "gaps" inherent in manual reports.

2. Change in Audit Firms – "new sheriff in town" mandates changes

As reported by the Public Company Accounting and Oversight Board (PCAOB), the Big Four accounting firms turned in twice as many deficient audit reports in 2010 as compared to 2009 (Compliance Week, December 22, 2011). While "lack of proper internal controls" is just one reason for a deficient audit report, we have found that accounting firms are demanding a lot more of their clients, specifically in SoD compliance.

For example, one SAP customer we worked with found their new audit firm wanted quarterly SoD reports out of all of their SAP applications whereas the former auditor only wanted semi-annual reports from just their core ERP production system. In other words, the new audit firm required an eightfold increase in effort!

Auditors are also more application savvy. In the past they may have been satisfied with a manually prepared report, they may now insist on logging into systems and running on-line queries. In the past, audit attention may have been limited to primary production systems may now include ancillary and development systems – as we saw with our customer.

3. First generation GRC solution is inadequate

First generation GRC solutions were often implemented between 2003- 2007 and are typified by high-level of maintenance, hard-to-use reporting, dedicated hardware, and limited functionality.

Some enterprises who have implemented a "first generation" SoD compliance reporting solution are facing an expensive an upgrade or a reimplementation of their solution. As all enterprises consider the total cost of ownership (TCO) of existing solutions – or total cost of compliance (TCC) - many decide to evaluate more efficient, cost effective solutions.

ControlPanel GRC

SYMMETRY™

4. A negative audit finding necessitates a change

A negative audit finding can certainly create a "tipping point" to find a new solution. Boards take audit findings very seriously and an adverse finding can effect shareholder value and damage careers. We have found that many organizations don't want to wait for a negative audit to change their SoD compliance strategy, but in some cases, it becomes an unsavory catalyst for a change.

5. A "near miss" or bona fide incident occurs, resulting in a need to change

In addition to creating problems for compliance reporting, poor SoD controls increase the enterprise's risk of genuine fraud or inadvertent mistakes that can affect normal business execution.

Sometimes enterprises experience a "near miss" where it is discovered that inappropriate access within their ERP, or system of record, could have (but didn't) cause a significant problem. Other enterprises actually experience a bona fide incident of fraud or theft of confidential data.

Well publicized incidents within an industry or in nearby companies, often cause executives to start asking questions.

What to do next?

Enterprises live with business problems all the time. Most are relatively easy to surpass, often with the day to day heroics of dedicated staff. However, when the impact of a business problem increases to the point where it becomes a significant risk or impediment to achieving business objectives – or an individual decides "enough is enough" – an organization will work to resolve the problem. The five aforementioned reasons often create triggers to investigate a new approach to SoD compliance and reporting.

When the tipping point is reached and firms decide to search for a solution to their SoD controls and compliance reporting business problem, the first option to consider is whether their existing solution can be scaled or fixed.

In the case of manual SoD compliance reporting, adding additional staff or outsourcing the task to a third party vendor are options, although in a postrecessionary environment, most enterprises are loath to increase staffing.

However, in our opinion, SoD reporting in SAP (which is our focus) for audit and compliance can become too onerous using current manual or semiautomated solutions. Preparing reports can be weeks if not months of labor. The results of manually prepared reports may be subject to further scrutiny requiring additional rework. The time and distraction from other more value add work by staff while preparing SoD compliance

ControlPanel GRC

SYMMETRY™

reporting incurs quantifiable opportunity cost, whereby other initiatives are delayed or additional staff is required to be hired.

For organizations looking at upgrading or replacing a current first generation SoD compliance reporting solution, the opportunity to reduce the costs of annual software maintenance, server infrastructure and administration costs must be considered. In addition, many organizations using an existing solution are facing an expensive upgrade or re-implementation and possibly additional licensing costs.

Beyond quantifiable costs, coping with the current methods is complex, distracting, and can frankly lead to embarrassment. Compliance, IT and internal audit teams pride themselves on thoroughness, high ethical standards, and quantifiable measures. An inability to provide accurate, complete data in a reasonable timeframe creates a lot of stress and tension on these teams. While it's hard to measure the "cost" of this emotional impact, it's a factor that should not be ignored in evaluating new SoD options.

In the case of the aforementioned SAP customer facing increased reporting requirements due to a change in external auditors, total staff hours were to increase to over2900 hours per year. Estimating a burdened cost of $50-70 per hour for IT security staff, the new audit requirements could cost $145,000-203,000 per year in labor. Since the SAP security team is also required to support on-going SAP projects and roll-outs, the lack of resource availability without hiring or retaining expensive external consulting resources would result in delays in those projects. Ironically, the time required to create SoD compliance reporting also detracts from the time available to be more aggressive on actual risk mitigation and maintaining a better SAP security architecture.

TCO or TCC costs for a new SoD compliance reporting solution include the software licensing costs, annual software maintenance fees, incremental IT infrastructure (equipment, maintenance and administration), and implementation costs. These costs must be compared to the on-going costs of the current methods.

Our recommendation is to initiate analysis that includes: 1) analysis of current time/costs of SoD compliance reporting, 2) required SoD functionality for your organization, 3) auditors recommendations; 4) analysis of GRC software solutions; 5) TCO or TCC costs.

Checklist of SoD solution functionality

Common "must have" features of a SoD solution include:

- **Embedded compliance** - Compliance data is automatically captured and stored on-line which provides the ability to produce ad hoc and on-demand reports.
- **Easy and intuitive graphical user interface** – Ease of use is critical because it enables the solution to be adopted by business users without having to engage IT

ControlPanel GRC

SYMMETRY

to provide answers to simple questions. Intuitive dashboards that allow users to drill down for detailed data are also important.

- **Audit ready reporting** - One of the factors that cause manual and semi-automated approaches to SoD compliance reporting is the need to perform several data transformations to get a useful report. A solution should not require "pivot table" hell to provide needed results. Also, it should be formatted with information the auditors expect.
- **Easy Reporting** – Can be quantified by time spent creating reports. We believe that it should be less than 8 hours a month.
- **Enable business users to self assess for risk** - Additional functionality provides a sounder SAP security architecture.
- **Real-time analysis of SoD data** – We believe sample data doesn't give an adequate view of real risk. Where it can, we believe real-time, actual data should be leveraged to report on real SoD infractions and issues.
- **Continuous control monitoring** – Monitoring and having exceptionbased reporting is important because it provides alerts when users execute conflicting portions of the same business transaction.

A User's Perspective:
Chad Wyckoff, Director, Security & IT Risk Services Forest City

"ControlPanel[GRC] has enabled our SAP Security and QA/QC teams streamline its current manual IT processes and controls through automation. The SAP Security team is now able to centrally automate approval workflow for user account/role maintenance requests for all SAP clients and integrate SoD assessments with these requests. ControlPanel[GRC] has also reduced the SAP security monitoring controls from 400 hours per quarter down to 8-12 hours. Associates no longer have to call the Help Desk to reset their password or manually setup the same passwords across the multiple SAP clients. This is all handled through self-service features provided to us by this product. Finally, we have been able to automate our transports between clients once the required approvals have been obtained via the automated workflow approval. This solution has enabled me to realign resources from very tactical activities to more strategic enterprise projects.

About Forest City

Forest City Enterprises, Inc. is an NYSE-listed national real estate company with $10.5 billion in total assets. The company is principally engaged in the ownership, development, management and acquisition of commercial and residential real estate and land throughout the United States. For more information, visit www.forestcity.net

About ControlPanel[GRC]

ControlPanel[GRC]™ is a new breed of Governance Risk and Compliance (GRC) automation solutions – one that focuses on rapid implementation, ease of use and broad functionality aimed at making SAP® users Always Audit Ready™. Part of Milwaukee-based Symmetry Corporation, ControlPanel[GRC]'s integrated GRC technology suite addresses the major areas of compliance concerns for SAP users. With over 50 implementations in two years, ControlPanel[GRC] has given its clients the ability to confidently satisfy compliance requirements while accelerating workflows that enhance their team's productivity.

For more information about ControlPanel[GRC], visit Symmetrycorp.com or call 1-888-SYM-CORP.

Always Audit Ready™

Summary

A lot has happened in the ten years since SOX legislation was passed. While almost all public companies are compliant with SoD requirements , for many it has become unmanageable. In most cases, "first generation" GRC tools and manual processes are not able to keep up with auditor demands in 2012.

There are various "triggers" or reasons organizations shift course and look of new SoD compliance automation solutions and strategies. In most cases, reviewing TCO of current solutions versus expected TCO of other options is part of every evaluation process. It's also important to list the critical functionality that needs to be part of your new SoD compliance reporting.

About ControlPanel[GRC] Segregation of Duties Solutions

Our solution allows users to identify, remediate and mitigate SoD risks before making changes in their SAP® production systems. It also helps maintain a clean environment with tools for ongoing monitoring and exception based reporting of executed risks.

Identify: SoD Risk Identification

ControlPanel[GRC] delivers a complete "risk based" set of the segregation of duty rules in SAP that are common to all industries and based on industry best practices. Our solution provides a detailed, plain English description of the potential risks, the reasons for the risk, and all remediation and mitigation options.

Analyze: SoD Risk Modeling

ControlPanel[GRC] provides strong "what if" modeling capability that allows for real time modeling of all requested user and role changes prior to the change actually being implemented. This functionality allows users to stay "clean" by identifying SoD risks and remediating or mitigating them on a continuous basis.

Monitor: Real-time notification of SoD issues in SAP

ControlPanel[GRC] is the solution for managing segregation of duties risks in real-time. The solution focuses on continuous controls monitoring for SoD – finding real risks when someone executed conflicting portions of the same business transaction. It also provides an in-depth review of executed risks and provides details on which transactions were executed and when.

Remediate and Mitigate: Fast Solutions for Risk Reduction

ControlPanel[GRC]'s detailed reports provide people in the business, the true risk owners, with all the information necessary to make judgments on appropriate remediation or mitigation options and then take action.