ControlPanel GRC

SYMMETRY™

CONTROLPANEL[GRC] ALWAYS AUDIT READY™ SERIES:

Companion Suite

How to extend and complement prior GRC Investments in SAP®

How ControlPanel[GRC]'s Companion Suite Helps Answer Today's Top Auditor Questions

Every year, internal and external auditors are broadening their scrutiny of IT controls over critical processes, including controls within the enterprise's Enterprise Resource Planning (ERP) financial system of record, which for many enterprises is SAP.

In an effort to comply with the 2002 Sarbanes-Oxley (SOX) legislation, many enterprises invested in first generation ERP GRC software tools. Because SOX had a clear focus on Segregation of Duties (SoD) controls, most compliance automation software also had a SoD focus. However, a lot has changed in the past ten years. There's an increased recognition among boards and auditors that other areas of IT operations also present significant risk to the enterprise. Recognizing that immediately implementing broad, rigorous IT controls is not feasible, auditors have adapted a measured approach whereby every year the scope and depth of IT audits increase. Even with this staged approach, many companies struggle to keep up with the

ControlPanel GRC

SYMMETRY™

increased changes, creating extra manual processes or “band-aid” fixes to their existing GRC solution.

Audit scrutiny regarding SoD has also not diminished. Auditors used to be satisfied with point in time samplings to determine the effectiveness of preventative controls in SoD. Increasingly, auditors are asking that “alwayson” detective controls are in place to determine if infractions have occurred, in real time. This approach to controls is called Continuous Controls Monitoring (CCM) and is a hot area in IT audit. First generation GRC software tools were designed for “point in time” reporting and post facto sampling of data. Next generation GRC solutions now address CCM requirements directly.

A Fork in the Road

The change from auditor/regulatory requirements from 2002 to 2012 has forced many companies to reevaluate their compliance programs, processes and software. To contend with increasing auditor requirements, businesses have a number of options:

- Hire additional internal staff
- Outsource operations to third party compliance reporting services
- Upgrade/re-implement existing GRC solutions
- Implement point solution GRC software to augment existing software
- Customize existing IT applications to support (e.g. helpdesk software)
- Adopt next generation GRC software solutions

All of these options have merits depending on a company’s particular situation. Typically, upgrading an existing solution, replacing it with a new GRC solution or implementing a point solution that augments existing GRC software are the three most common choices. Hiring internal staff and outsourcing options tend to not be selected because companies do not want to increase annual operational expenditures. Another option not typically selected is customizing IT applications to support GRC activities because it causes operational hassles and creates an endless cycle of support and maintenance.

Deciding whether to upgrade, install a new solution or add a point solution comes down to two key factors - cost constraints and functionality requirements. For most companies, the idea of a modular, yet integrated, solution is most appealing to them. Determining the right approach for an organization typically depends on how a company plans to answer a series of questions related to the new areas of compliance and auditor focus in 2012. If your auditors haven’t asked you for more documentation in the following areas, it’s likely they will in the next year or two.

Compliant user provisioning

Effective SoD controls help mitigate the risk of a single employee performing a sequence of transactions for fraud. However, auditors are increasingly looking for

ControlPanel GRC

SYMMETRY™

controls around the processes of creating, changing and deleting the User IDs in critical IT systems. For many enterprises, the current audit trail for user provisioning is a combination of emails, helpdesk tickets and application logs. The process for creating compliance reporting is manually assembling the documentation from multiple sources, typically manually compiled sampling periods.

How do you respond if your auditor asks you:

- Who requested a User ID change (add/change/delete)?
- Who approved the change?
- What was changed?
- When was the change made?

Compliant role change management

Poor role administration in SAP is a breeding ground for segregation of duties violations. Plus, auditors are becoming more application savvy and are asking for log on rights to the applications themselves. Regarding role change management, auditors have become more aggressive in flagging poor or degrading SAP security role architectures.

How do you respond if your auditor asks you:

- Who reviews role Assignments?
- How role assignments to User IDs are assigned?
- Who approves role definitions?
- Tell me what roles were assigned to what users since…

Transaction usage analysis

Increasingly, auditors are changing their stance on risk mitigation. The focus is changing from preventative controls – mitigating the risk of something bad from occurring – to "detective controls" – reporting in real-time that something bad has actually happened. Board of Directors are also requiring this data from SAP in order to have evidence of fraud or malfeasance.

Native functionality in SAP does not record comprehensive data on user sessions, just basic time stamping on login/logouts. Attempting to mine forensic data of actual systems usage is difficult. Custom programming or third-party tools are usually required.

How do you respond if your auditor asks you:

- Can you confidently report in real-time on fraud or wrong-doing in SAP?
- Could rigorous transaction usage capabilities aid with productivity or performance of your internal audit or finance group?

ControlPanel GRC

SYMMETRY™

Privileged user access

SAP users pssoessing privileged "super user" access rights in SAP have the ability to possessing, delete or alter sensitive data within the enterprise's financial system of record. Sometimes it is required to grant super user access to override functions in order to correct emergency issues or perform nonstandard maintenance. Auditors now want to know what super users, or system administrators, are doing in SAP, not just end-users.

How do you respond if your auditor asks you:

- Can you track when emergency privileged access was granted and what they did?
- Do you have an automated report on emergency access sessions?

Compliant transport management

There are several factors that cause stress on the change request, or transport management process, in SAP – manual controls and intervention, overlapping change requests, sequencing issues, and multiple development and production environments. And if SAP is "stressed" due to a transport, there is a risk that the whole enterprise will go down. Plus, auditors are causing yet another stressor for SAP administrators as they demand demonstrable controls of the SAP change request/transport management process.

- How do you respond if your auditor asks you:
- Can you provide automated reports on transports?
- Is the transport management process automated – including testing and sequencing?

Compliant batch management

While primarily an online transaction processing (OLTP) environment, most SAP customers have critical data processing that is run in batch jobs using SAP's native batch management functionality. However, auditors are now questioning the actual performance of batch processing, especially those that impact financial data.

- How do you respond if your auditor asks you:
- Who approved the execution of a batch run?
- Who reviewed the batch execution code?
- When was a batch job run?
- Were there any errors? If there was an error, how was it resolved?

Business process controls

An emerging area of focus for auditors is business process monitoring (BPM). Unlike the other "new" categories of auditor focus, BPM isn't IT-focused, but is more business-related. Finance managers (and auditors) are looking for ways to get reporting on

ControlPanel GRC

SYMMETRY™

exceptions of normal business processing and business practices. For example, if there is a policy that no purchase order over $50,000 can be processed without secondary approval, are there any violations to that policy?

How do you respond if your auditor asks you:

- Do critical financial processes including procure-to-pay and order-tocash have automated tracking in place?
- Can you track if policies have been violated? What is the level of effort required to track those violations?

A new era of compliance reporting

The difference in compliance reporting from 2002 to 2012 is stark. However, there's no reason to be caught flat-footed in any of the new areas of increasing auditor focus. Software and process updates exist to help you contend with automated reporting and tracking of:

- Compliant user provisioning
- Compliant role change management
- Transaction usage analysis
- Privileged user access
- Compliant transport management
- Compliant batch management
- Business process controls

ControlPanel[GRC] is one option to help you with the new compliance requirements. While the solution can be implemented as a standalone solution, we also offer a Companion Suite that extends and complements existing SAP or other SAP-related compliance software options. Being Always Audit Ready™ today doesn't need to be scary, hard or expensive. We believe in providing user-friendly tools that can be implemented in a short period of time (often a week or two) at a fraction of the cost of other solutions. Moreover, we also have a number of operational efficiency functionality in our Companion Suite to help you reduce your total cost of operations from your SAP investments.

The following checklist helps parse out the new areas of auditor focus and demonstrates how SAP and a solution like ControlPanel[GRC] can work together to make you Always Audit Ready.

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.

Compliance Automation Funtionality	SAP GRC	ControlPanel[GRC] Companion Suite
SoD Analysis (Risk Analyzer)	√	
Role Management (User and Role Manager)	√	
Compliant Role Change Management (User & Role Change Manager)	√	
Privileged User Access (Emergency Access Manager)	√	
Process Controls (Process Analyzer)	√	
Continuous Controls Monitoring for SoD (Risk Analyzer)		√
Compliant Transport Management (Transport Manager)		√
Transaction Usage Analysis (Usage Analyzer)		√
Compliant Batch Management (Batch Manager)		√
Operational Efficiency Funtionality	**SAP GRC**	**ControlPanel[GRC] Companion Suite**
License Optimization (Usage Analyzer)		√
Password Management (Password Manager)		√
SU53 Security Issue Resolution (Security Troubleshooter)		√
Automated Testing (Security Quality Assurance)		√
Role Versioning and Roleback (User & Role Change Analyzer)		√

Always Audit Ready™