



Rick Killpack
Senior Product Manager
Identity and Security
Novell

Compliance: Bane or Benefit?

Finding Compliance's Silver Lining

The demands of regulatory compliance are not going away. In fact, they're steadily increasing. But while attaining and proving regulatory compliance can seem like a grueling process, there is an upside: The long, hard look at the business, how it functions, and all of its associated workflows – a prerequisite of any successful governance, risk, and compliance (GRC) effort – can be leveraged beyond simply meeting regulatory compliance; it can be extended to reduce risk and build operational efficiencies. To achieve these added benefits, companies first need to ask themselves:

- Do we have the right business processes in place?
- Do our IT investments support those business processes?
- Where are our unnecessary risks?
- How can we contain costs to drive revenue growth?

None of these questions can be answered by considering each issue independently; they're all interrelated. At a high level, processes (such as those for access control) are defined to achieve specific business goals. However, implementing those processes and keeping them well tuned requires technology and effort. Furthermore, technology should not only streamline business processes, but also minimize risk exposure and eliminate unnecessary costs.

For most organizations, this is easier said than done. The IT infrastructure often ends up looking more like a patchwork of disparate technology than a well-designed quilt. Consider the common process of moving an employee from one role to another. During this change process, managers must ensure that the employee's access to systems and resources mirrors the changes in his or her role.

This is where complexity creeps in: The employee's role-based access spans multiple SAP applications as well as infrastructure that extends beyond SAP. For each system, a unique set of technical roles, entitlements, and policies must be maintained. The result is a set of dissimilar provisioning and access control systems that increases costs, impedes

compliance efforts, introduces complexity, creates security loopholes, and provides little visibility into who has access to what resources. So how can a firm ensure consistency between SAP and other systems? By integrating that unique set of roles, entitlements, and policies across enterprise systems.

Building the GRC Bridge

SAP BusinessObjects governance, risk, and compliance (GRC) solutions provide full GRC coverage for SAP applications. These solutions help companies manage risks, governing processes, and access control over business applications. However, enterprises can't effectively mitigate risks to these critical business applications without enforcing security controls within the underlying IT infrastructure of those applications – as well as in the rest of the infrastructure.

To achieve this rock-solid security and enforcement, Novell has extended its Compliance Management Platform (CMP) to integrate with SAP environments. The platform helps companies streamline security and regulatory compliance efforts and reduces redundant manual efforts and associated security spending.

The Novell Compliance Management Platform extension for SAP environments unifies user provisioning, access control, and security event monitoring for non-SAP applications and IT infrastructures into a single comprehensive platform along with SAP BusinessObjects GRC solutions. By doing so, it helps clients make certain that:

- Users have access to only the appropriate resources
- Users' digital identities are managed properly throughout their life cycle as job roles change
- Meaningful security events are identified to the appropriate managers – or even remedied automatically

Novell's CMP solution delivers a unified, real-time view of user activities and notable security-related events (systems falling out of their secure configuration, for example) across critical applications and systems within the enterprise

SAP has recently certified Novell's CMP extension for SAP environments with SAP BusinessObjects Access Control, SAP ERP, and SAP NetWeaver.

(see **Figure 1**). These activities are correlated with existing processes and controls to identify IT risk exposures and manage remediation efforts. This process streamlines security and regulatory compliance efforts: It cuts compliance-related costs by minimizing redundancies and security loopholes in processes throughout the enterprise.

The Solution in Action

When it comes to provisioning and identity and access management, the complexity lies in the multiple, uncorrelated systems used to manage access and provisioning for new hires, role changes, and terminations.

Consider this example: Let's say an employee is changing roles from an accounting clerk to an accounting manager. For her new role, the accounting manager must have access to a new set of resources. In addition, maintaining the appropriate separation of duties at all times is crucial. For

FIGURE 1 ► The CMP solution's unified, real-time view of user activities and security-related events



Getting Started: Establish Your Baseline

More often than not, enterprises need experienced and proven guidance to help them integrate their siloed security and compliance efforts. Deloitte & Touche LLP delivers this knowledge and experience – helping SAP customers evaluate how entitlements and access management are handled both in their broader infrastructure and within their SAP environment.

Deloitte & Touche LLP's mature delivery skills and tools help clients create a baseline of their existing situation and build a roadmap to coalesce the way identities are managed across applications and systems – including SAP systems. This helps companies manage costs, reduce their regulatory burden, and increases security effectiveness.

this, her organization needs to provide and track access, and instantly identify and provide alerts about any policy violations, such as gaining access to both the accounts payable and receivable systems.

Properly setting up the accounting manager requires a strategic layering of technology, such as SAP BusinessObjects Access Control and the Novell Compliance Management Platform extension for SAP environments. This pairing helps companies ensure that business policies will be consistently enforced and monitored across SAP and non-SAP applications throughout the organization.

Why is this so important? Because managing at this level of maturity is crucial for cost-effective governance, regulatory compliance, and the security of systems and data. Just consider the sheer number of security breaches that have been disclosed publically. Almost every day, another firm or agency becomes snarled in a new data breach incident. Unfortunately, these incidents are on the rise. The Open Security Foundation and DataLossDB (www.datalossdb.org) identified 467 corporate data loss events in 2007, and that figure climbed to 644 last year. Today's siloed approach to compliance and security just isn't getting the job done.

Fortunately, by integrating the SAP environment with the rest of the infrastructure, enterprises can stay one step ahead of potential risks and growing compliance requirements. Rather than keeping security and compliance data in individual silos (or simply throwing technology or people at the problem), companies can monitor and manage this data and enforce the controls and processes that support standards and policies centrally across multiple business units, geographical areas, and the entire IT infrastructure.

Pulling the Pieces Together

By managing security and compliance efforts centrally across all applications and their underlying IT infrastructure, enterprises can eliminate redundant and poorly conceived compliance and security practices. This not only cuts cost, but enhances an organization's security and compliance posture.

Forward-acting organizations are moving away from tactical, ad hoc security and compliance management to a unified, sustainable management framework, which secures all business-technology systems and achieves compliance more efficiently. These companies realize they have to knock down their diverse silos and manage all identities, applications, security, and compliance policies centrally across the infrastructure. The firms that were breached last year clearly wish they had. To learn more, visit www.novell.com/cmssap. ■