

Improve Compliance Across SAP* and Non-SAP Systems

Table of Contents:

2 Rising Risk, Rising
Compliance Cost

3 The Solution: Novell
Compliance Management
Platform

5. Streamlining Communication
between Compliance and
Security Systems

6 A Real-time, Holistic View

8. The Platform in Action

10 Why Novell?



Rising Risk, Rising Compliance Cost

By blending its award-winning identity, access and security management technology, Novell has created the Novell Compliance Management Platform, an innovative solution that ensures that business policy becomes automated IT practice.

¹ IDC "Identity and Security Management and Strong Information Technology Governance: Novell's Solution Suite Automates the Approach to the Perfect Union." Sally Hudson, February 2008

For millions of people around the world, January 24, 2008 began like any other day—an ordinary Thursday in the middle of an average week. But for Société Générale, the second-largest bank in France, that particular day was one of sobering revelation. It was on that day that the bank announced it had been the victim of a US\$7 billion crime.

In an announcement reported around the world, bank officials revealed that, over the course of several years, a rogue trader executed fraudulent transactions that cost the bank billions of dollars. According to company executives, it was the trader's knowledge of internal policies and process controls that had allowed him to hide the fraud for so long. Though Société Générale reacted quickly to the discovery, dismissing related personnel and addressing recovery plans with investors and the media, the staggering losses significantly diminished the company's profits, shook customer and investor confidence and left the bank in the unenviable position of being the victim of the single largest act of fraud by an individual in the history of the securities industry.

Although the fraud discovered at Société Générale is one of the most dramatic examples of what can occur when corporate policy is breached, it is certainly not unique. Today, companies around the globe struggle to achieve compliance with internal policies and external regulations, expending enormous resources only to end up with a piecemeal solution that may get them through this year's audit but will likely be woefully inadequate at tackling tomorrow's threat. Companies implement SAP* GRC solutions to ensure that at least one part of their IT infrastructure meets internal and external needs, but strug-

gle to achieve the same peace of mind with the rest of their IT landscape. Even as compliance spending continues to increase dramatically year after year, analyst firms like IDC report that "inadequately addressed compliance regulations will result in increased violations and subsequent legal and public relations problems for corporations over the next several years."¹

Further complicating the matter, business executives must now take personal responsibility for compliance issues. An organization's failure to comply with established policies—whether internal or regulatory—could be damaging not just to the company's brand and image, but also to the personal credibility of the management team.

Amid such a challenging business climate, executives are left to ponder several pressing questions:

- *How can I offset the escalating costs required to achieve compliance?*
- *Can we integrate SAP policies and roles with other applications to automate key business processes?*
- *Do we know with confidence our compliance status at any given moment?*
- *Do our IT policies and infrastructure support our business goals and compliance requirements?*
- *How do I efficiently and effectively integrate the SAP and non-SAP environment to create a comprehensive compliance solution?*

Integrating SAP into Your Identity, Access and Security Ecosystem

Implementing an SAP security model presents a unique set of challenges. For example, how do you utilize employee data in SAP HR

to determine access policy to various SAP and non-SAP applications? Should you implement Common User Administration (CUA)? What impact will that have? How do you effectively manage passwords across SAP and non-SAP applications while enforcing password policies and providing password self service? Perhaps most importantly, how does your SAP security model align with your enterprise security and access strategy? These challenges and many others negatively impact business agility and the effectiveness of your corporate governance efforts.

Addressing Potential Threats As They Occur

Integrating security events between SAP and the vast array of other systems in your enterprise is another challenge that the Novell solution addresses. The Novell® Compliance Management Platform extension for SAP environments includes certified connectivity to the SAP Computer Center Management System (CCMS), allowing your organization to easily incorporate SAP security events with other network and application security events across the enterprise. This provides the validation you need to ensure that established governance policies are being followed, and that users have the right level of access to the right resources. Any anomalous activities, such as abnormal user access requests, are identified in real time. The solution then responds to the threat immediately. It can issue alerts to administrators, block user accounts or even shut down affected systems.

Delivering Role-based Access to Resources

The complex array of SAP roles, composite roles, profiles, portal groups and entitlements have to be managed and integrated with other enterprise applications. And it's a challenge to incorporate the various access and transactions afforded by these entitlements. The Novell solution simplifies these tasks with the Novell Identity Manager Role Mapping

Administrator—a component of the Novell Compliance Management Platform extension for SAP environments. This industry-unique, business-level interface enables IT security staff, provisioning system administrators and SAP business owners to collaborate on easily and quickly matching enterprise provisioning roles with the appropriate entitlements in SAP. With an interface that displays information in terminology familiar to each user, the Role Mapping Administrator allows you to automate the provisioning of SAP entitlements.

Simplifying Password Management

Anytime users have to manage multiple passwords across various SAP and non-SAP applications, administration costs rise and productivity decreases for both end users and IT staff. The Novell solution addresses this challenge by incorporating enterprise password management, including password self-service, to SAP and non-SAP applications throughout your organization. Now, users can have a single, strong password for accessing their applications. The password self-service capabilities in the Novell solution allow users to reset their passwords and visually confirm the password change, eliminating any questions about which applications' passwords are reset and ready for use.

The Solution: Novell Compliance Management Platform

Fortunately, as many companies around the world have already discovered, the tools and expertise to solve many of these challenges can be found in a solution offered by a company with decades of experience tackling the issues of security and policy enforcement. By blending its award-winning identity, access and security management technology, Novell has created the Novell Compliance Management Platform, an innovative solution that ensures business policy becomes automated IT practice.

The Novell Compliance Management Platform extension for SAP environments adds SAP-specific capabilities as the hub of automated identity, access and security management features of the Novell Compliance Management Platform.

By extending user provisioning, access control and security monitoring across SAP and non-SAP systems, the Novell Compliance Management Platform extension for SAP environments delivers business process automation that gives users the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk.

The Novell Compliance Management Platform extension for SAP environments enables company executives to not only be confident in their compliance posture, but also trust that their image, brand and reputation are safe.

To support SAP-specific environments, Novell delivers the Novell Compliance Management Platform extension for SAP environments. This first-of-its-kind technology leverages SAP HR data (or other appropriate authoritative sources) to automate user provisioning for any number of SAP applications directly, or through integration with CUA. It also distributes identities to non-SAP applications throughout the enterprise.

The Novell Compliance Management Platform extension for SAP environments leverages the policies and practices your organization has established in your SAP environment and provides the foundation to integrate them with the rest of the IT landscape. Similarly, policies and practices established outside the SAP environment can be extended to the

appropriate SAP applications. The result: Organizations can gain additional leverage from their SAP investments while enhancing organizational efficiency and security. The Novell Compliance Management Platform extension for SAP environments enables company executives to not only be confident in their compliance posture, but also trust that their image, brand and reputation are safe.

To understand the urgency of deploying such a solution, it is important to consider why compliance is so difficult to achieve in the first place, and why thousands of companies are at risk from internal and external threats despite spiraling budgets.

Extend Identity, Access and Security Across IT Systems



Figure 1. Extends roles provisioning between SAP and other IT systems

Streamlining Communication between Compliance and Security Systems

IT has become the cornerstone of most organizations' efforts to achieve compliance, with the primary goal being the automation and enforcement of policies originally developed on paper. The most important product categories to emerge in the fight to enforce policy are identity and access management, and security information and event management (SIEM). Identity and access management products determine users' identities and then grant and revoke appropriate access to corporate applications, while SIEM solutions provide an enterprise-wide view of perimeter security and other products, including intrusion prevention systems and firewalls. In short, identity and access management specifies who *should* have access to corporate resources, SIEM identifies who *is* accessing corporate resources—both of which are integral components of policy and regulatory compliance.

The key is to leverage identity and access technologies with a SIEM solution, maximizing existing investments to make achievable, scalable, forward-looking compliance a reality. According to IDC, the identity and access management market alone will reach US\$5 billion by 2011.² Why? Because compliance and corporate governance initiatives will continue driving the need for these capabilities.

Modern identity and access management products are extremely adept at validating identity, provisioning resources and enforcing access roles. Likewise, SIEM solutions do an excellent job of aggregating security data from across the enterprise. However, in most cases, these two technologies are not very good at working with each other. In many organizations, there are two silos of information: one that holds identity and access

management policies (who gets access to corporate applications) and another that contains security data (who is accessing corporate applications). As in the case of Société Générale, it is this "gap" between what should be happening and what is happening that provides an opening for criminal activity.

Consider this illustration to understand why the integration of identity and security management is so vital to achieve compliance: A typical financial transaction within SAP ERP may need to touch an in-house application and a transactional database before it is completed and funds are dispersed. Both the in-house application and the transactional database generate log data that is tracked by a SIEM system every time an action is executed on those applications. An employee with user access to the financial system and inadvertently granted administrator access to the in-house application could conceivably divert funds.

Ensuring that employees cannot circumvent the established process and initiate an unauthorized transaction is critical to avoiding criminally fraudulent activities within the organization. With no common framework to tie together the elements of the identity and security infrastructure, a perpetrator could commit a crime by taking advantage of his or her access to privileges or knowledge of internal processes.

Within SAP environments, difficulties can arise when SAP applications have to interact with non-SAP applications and technologies that do not have a common method for validating and enforcing policy. Further, some business-critical systems may never interact with the SAP systems, yet the need to enforce policy in those systems is also important. Fortunately, implementing policies and access rules across SAP and non-SAP systems is possible without requiring a costly re-engineering of the IT infrastructure.

Novell Compliance Management Platform extension for SAP environments ships out-of-the-box with integrated software as well as preconfigured identity and security policies and innovative best practices documentation. This gives companies a significant head start on developing compliance solutions that fit their unique business needs.

2 IDC "Identity and Security Management and Strong Information Technology Governance: Novell's Solution Suite Automates the Approach to the Perfect Union." Sally Hudson, February 2008

By blending its award-winning identity, access and security technology from the Novell Compliance Management Platform with new technology created specifically for SAP customers, Novell has delivered the ultimate governance solution.

Bridge the Gap Between Disparate Enterprise Systems

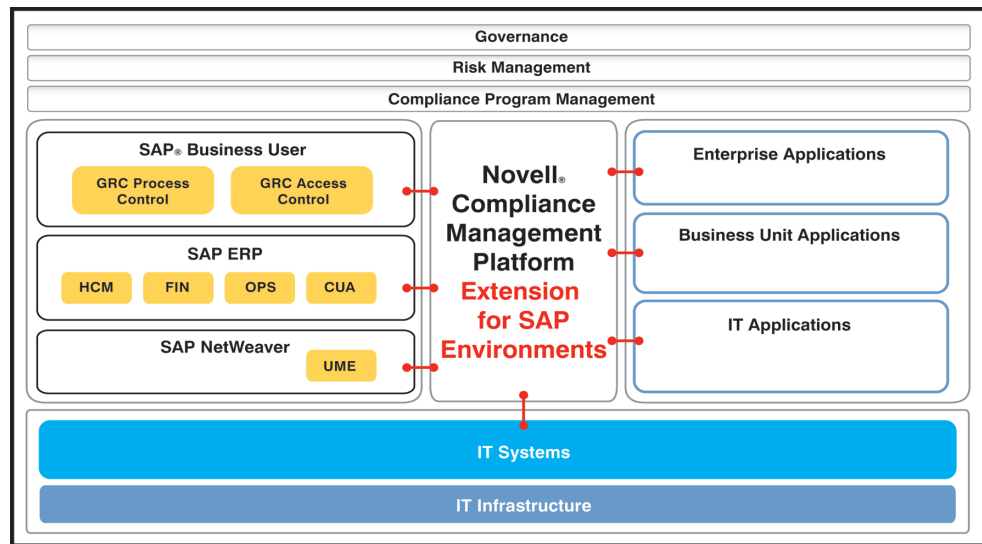


Figure 2. Supports integrated, enterprise approach for managing user access risk and compliance across SAP components as well as the broader IT landscape

A Real-time, Holistic View

Bridging the gap between identity and security, the Novell Compliance Management Platform extension for SAP environments provides a real-time, holistic view of the enterprise and its compliance status. The Platform extension cross-validates identity, access and security information in real time across SAP and non-SAP systems, so the business always knows who is accessing what, when they are doing it and if they are authorized. In turn, if situations arise that are out of the norm, the Platform takes appropriate action in real time that can range from simple notifications to the initiation of full remediation (e.g., revoking user access). The actual “remedy” for the violation is determined by the organization.

By extending user provisioning, access control and security monitoring across SAP and non-SAP systems, the Novell Compliance Management Platform extension for SAP environments delivers business process

automation that gives users the appropriate resources, validated in real time, to ensure compliance with company policies—eliminating the gaps that have left so many companies at risk. Instead of complex (and expensive) product silos, Novell Compliance Management Platform extension for SAP environments delivers an enterprise-wide view and enforcement of policy as defined by corporate governance to SAP customers

At the heart of the Novell solution is its ability to operate in real time. No other identity, access or security management provider delivers a comprehensive solution that addresses both identity and access management and SIEM in real time for environments with SAP and non-SAP systems. While most identity management products take a periodic assessment of policy changes—creating a lag time between administrator actions (like revoking a disgruntled employee’s access to a financial database) and policy enforcement—the Novell solution implements policy changes as they occur.

Next, as policy and security data are gathered in real time, the Novell Compliance Management Platform extension for SAP environments correlates the information to identify legitimate threats. For instance, a user who legitimately logs in to (i.e., has a valid username and password) SAP ERP may simply be doing business as usual. However, if that user's role within the company does not warrant access to the application, that login could present a serious threat. The Novell Compliance Management Platform extension for SAP environments can correlate the application log data with provisioning policies to catch this kind of security risk, which could easily go undetected by a piecemeal compliance solution—that is, until the auditors decide to take a closer look.

Process Automation

In addition to correlating identity and security, automation is also a key factor in the Novell solution's ability to ensure compliance. Organizations are placing themselves at risk when they depend on manual processes to prove compliance. Any manual process introduces the possibility of human error, not to mention the possibility of willful misconduct, and increased expense.

Novell Compliance Management Platform extension for SAP environments can pinpoint areas of concern and notify the appropriate individuals about those concerns, taking the guesswork out of evaluating compliance. The Platform can even automate the process of provisioning access to corporate applications, based on a user's self-service request, if the request is in line with company policy. Again, the need for manual intervention, with all of its associated risks, is eliminated.

Finally, the Novell Compliance Management Platform extension for SAP environments is a completely integrated solution, built on industry-leading identity, access and SIEM technologies that work seamlessly together.

In fact, Gartner, Inc. recently called the Novell suite the "most tightly integrated suite in the market."³ Other compliance-related offerings claim to be comprehensive solutions with strong returns on investment, but in reality they are little more than a set of unintegrated products that create additional silos in the organization.

Deploying these piecemeal "solutions" requires substantial effort to assemble, correlate, and integrate SAP and non-SAP policies. In contrast, the Novell Compliance Management Platform extension for SAP environments ships out-of-the-box with integrated software as well as preconfigured identity and security policies and innovative best practices documentation. This gives companies a significant head start on developing compliance solutions that fit their unique business needs. Better still, the Novell Compliance Management Platform extension for SAP environments allows companies to begin realizing a higher return on their SAP investments.

Solution Benefits

As the ultimate governance solution, the Novell Compliance Management Platform extension for SAP environments delivers many compelling benefits:

1. The Platform extension has preconfigured policies and documented best practices created specifically for companies with SAP solutions. These allow your organization to address GRC requirements through the alignment of roles and entitlements between SAP and other systems.
2. The Platform extension minimizes the anomalies, uncertainties and violations that can ruin a company's reputation. Its real-time capabilities provide the information needed to instantly remediate any divergence from business policy both inside and outside SAP solutions, assuring that little or no damage is actually done.

Novell Compliance Management Platform extension for SAP environments provides a real-time, holistic view of the enterprise, leverages your existing SAP GRC investments, mitigates the risks posed by internal and external threats, and ultimately ensures that your organization's image, brand and reputation are safe.

³ Gartner, Inc. "Comparing IAM Suites, Part 1: Suite or Best of Breed?" Earl Perkins, March 2009

The Novell Compliance Management Platform extension for SAP environments extends the same processes to SAP systems and other applications across the organization, thus reducing the complexity and cost of identity management and security.

3. Rather than requiring administrators to separately manage point solutions, the Platform extension provides one central point for managing the entire identity, access and security management infrastructure. This significantly reduces costs and ensures consistency and reliability enterprise wide.
4. The Platform extension provides improved security to SAP customers by automating enterprise provisioning activities while at the same time validating users' access to all company systems. By combining these two critical components of compliance management, your organization can address critical issues such as separation-of-duties policies, while simultaneously ensuring compliance to internal policies and external regulations.
5. The Platform extension allows organizations to rapidly react to the changing business environment in a secure and agile way. Whether it's bringing on new partners or absorbing new employees from an acquisition, the systems remain secure while the business process needs are met. The reduction in time to integrate these changes can have a huge impact on the bottom line.
6. User interactions with the Platform extension will promote trust. Rather than requiring a call to the helpdesk for password support, the Platform's self-service password maintenance lets the users manage their passwords for all corporate resources via a user-friendly graphical interface that will visually indicate which systems were affected by the change. In addition, users can initiate a self-service request to be provisioned access to a key SAP or non-SAP application. That request can then be automatically approved if the user's identity and role match the corporate policy for access to the application.

With these high-level benefits in mind, it's valuable to take a closer look at how the Novell Compliance Management Platform extension for SAP environments can be applied to several typical scenarios throughout the enterprise.

The Platform in Action

A comprehensive approach to compliance addresses both inadvertent breaches of policy as well as acts of willful misconduct, as in the following illustrations:

Role-based Provisioning

Role-based provisioning automates the process of granting appropriate access to resources based on users' roles. The Novell Compliance Management Platform extension for SAP environments extends the same processes to SAP systems and other applications across the organization, thus reducing the complexity and cost of identity management and security. Our solution provides a way for IT administrators, security officers and SAP application owners to quickly and easily integrate SAP roles, composite roles, profiles or groups with the roles defined within the provisioning system.

If your company is in a high-security industry, such as health care or financial services, you can ensure that access rights for role memberships are managed properly so you will always be in compliance with internal and external regulatory standards. Because access to resources is based on roles and policies that are consistently enforced, role-based provisioning from Novell increases the security of your valuable IT resources while making it easy to prove compliance with government and industry standards.

Identity-enriched Security

By mapping security information to identity profiles, the Novell Compliance Management Platform extension for SAP environments enables organizations to be much more effective at identifying and investigating security breaches. Without this correlation, if a user were to attempt to access a sensitive customer database in the SAP Business Suite by overriding security protocols, database administrators would know little more than the fact that someone tried to break in. Using the Novell solution, those same administrators could quickly turn to an easy-to-read, real time dashboard to determine who attempted the security breach, what else he or she had been doing recently and what other accounts that user has across the enterprise. This clear, graphical overview of identity and security concerns throughout the organization enables administrators to make sense of mountains of security data, identifying legitimate threats while eliminating false positives.

Rogue Administration

The Novell Compliance Management Platform extension for SAP environments guards against changes made by administrators that overtly or accidentally violate policy. For instance, a new accounting employee is assigned to work with the marketing department and is granted appropriate access to SAP ERP Financials. Then a system administrator—either intentionally or inadvertently—grants the new accountant additional access inside the financial application, giving him visibility into the finances of not just the marketing department, but the entire organization. With the Novell Compliance Management Platform extension for SAP environments in place, the inappropriate

access is not only immediately revoked, but the action is also correlated with relevant security data. This helps determine who it was that granted the additional access, so the appropriate security personnel can be alerted. Certainly, given the employee's job function, it is quite possible that the provisioning error was simply a mistake—but the Novell Compliance Management Platform extension for SAP environments gives companies the insight they need to make that determination for themselves before a more serious security breach can occur.

Provisioning vs. Utilization

SAP GRC solutions can identify which users are provisioned to which SAP applications. Other identity management systems can obtain the same data for non-SAP applications. But are those employees actually using the applications? That's a question that can only be answered when identity management and security management are correlated, as they are with the Novell Compliance Management Platform extension for SAP environments. Using the Novell solution, administrators gain an additional level of inspection and validation, which provides them visibility into not just which users have access to corporate applications, but also how often those employees log in to and use those applications. Tracking application usage is an excellent way to gauge whether corporate policies and role definitions actually line up with day-to-day operations.

Streamlined Access

The Novell Compliance Management Platform extension for SAP environments maximizes user efficiency because it automates the process of requesting application access. For example, a salesperson attempts

Novell expertise in compliance-related solutions is second to none. The company is not only an established leader in identity and security management, but is also a solution provider to thousands of organizations around the globe. That deployment experience allows Novell to go beyond just installing a patchwork of products. The Novell Compliance Management Platform extension for SAP environments combines powerful technology with preconfigured policies and documented best practices to provide a comprehensive approach to policy compliance—plus the most impressive return on investment available anywhere.

To learn more about the Novell Compliance Management Platform extension for SAP environments and how it can help organizations bolster security, boost performance and lower operating costs, go to: www.novell.com/cmepsap

www.novell.com

to log in to a new lead management system but is denied because access has not yet been provisioned. The Novell solution automatically determines if the salesperson should have access to the application, and if so, creates a workflow request. The request is then sent to an appropriate administrator. If the salesperson has already been granted rights to the SAP Account Management system, for example, then the same set of rights can be automatically extended to the lead management system. When the workflow request is approved, the user is provisioned to the application and notified. This self-service model not only improves the experience and the productivity of users, but it also serves as an additional layer of automation to ensure that policy compliance is maintained at a consistent level across all systems, and that it reduces the associated costs.

While these illustrations are in no way a comprehensive list of the capabilities of the Novell Compliance Management Platform extension for SAP environments, they do serve to demonstrate the scope of the Novell solution. Only by addressing such a broad range of challenges can the Platform extension actually ensure enterprise-wide compliance.

Customers can increase the value of their investment in SAP and address GRC

requirements with Novell Compliance Management Platform. The Platform:

- *Improves system security and audit quality throughout the enterprise.*
- *Enables customers to execute their GRC strategy through a robust identity and security framework without a significant increase in cost*
- *Provides sustainable compliance of access policies/controls throughout the enterprise*
- *Reduces compliance costs by sharing common identity data between applications and resources within the enterprise*
- *Maximizes SAP customers' compliance objectives through an integrated security framework designed to preemptively detect and remediate risks*

Why Novell?

By blending its award-winning identity, access and security technology from the Novell Compliance Management Platform with new technology created specifically for SAP customers, Novell has delivered the ultimate governance solution. This solution provides a real-time, holistic view of the enterprise, leverages your existing SAP GRC investments, mitigates the risks posed by internal and external threats, and ultimately ensures that your organization's image, brand and reputation are safe.



Contact your local Novell Solutions Provider, or call Novell at:

1 800 714 3400 U.S./Canada
1 801 861 1349 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.

404 Wyman Street
Waltham, MA 02451 USA



Novell.