

Security & Identity: A Winning Approach to Sarbanes- Oxley Compliance

How Integrated IT Controls and Monitoring Help You Succeed in Controlling the cost of Compliance

INTRODUCTION.....3

IDENTITY AND ACCESS MANAGEMENT’S ROLE IN COMPLYING WITH SARBANES-OXLEY.....4

NOVELL IDENTITY AND ACCESS MANAGEMENT SOLUTIONS.....6

 Novell® Identity Manager.....6

 Novell eDirectory™.....6

 Novell iChain®.....7

 Novell BorderManager®.....7

 Novell® SecureLogin.....7

 Sentinel™ 5.....7

 Novell® Storage Manager.....7

APPLYING NOVELL SECURITY & IDENTITY SOLUTIONS TO SARBANES-OXLEY.....8

ACHIEVING SUSTAINABLE COMPLIANCE AS A COMPETITIVE ADVANTAGE.....15

INTRODUCTION

Today's business environment is characterized by constant change, much of it driven by the need to comply with a host of government and industry regulations. Enterprises have no choice but to satisfy the requirements associated with these regulations, yet they must do so in the midst of resource constraints. In spite of the fact that budgets are already stretched thin, enterprises must find ways to respond to these increased demands. At the same time, organizations are attempting to juggle multiple objectives, such as complying with regulations to stay in business vs. focusing on strategic projects to get ahead of the competition.

The Sarbanes-Oxley Act (Sarbox) is a prime example of an information disclosure regulation that must be satisfied in order to stay in business. In order to fulfill Sarbox requirements, publicly-traded companies must generate accurate financial reports. Furthermore, they must enable auditors to understand and attest to how the company reliably initiates, authorizes, records, processes, and reports on its financial data.

Recently, the Public Company Accounting Oversight Board (PCAOB), which governs the Sarbanes-Oxley auditing process, issued clarification that helps organizations and auditors understand what to focus on in relation to ensuring compliance while minimizing auditing costs. PCAOB outlines a top-down approach that includes the following three steps: identify the points at which errors or fraud could occur in the process; identify controls to test that prevent or detect errors or fraud on a timely basis; and clearly link individual controls with the significant accounts and assertions to which they relate. These recommendations highlight the critical role that integrated and automated network monitoring plays in the compliance process.

A company's ability to address these requirements is closely linked to the security and access controls defined for its information technology infrastructure and business applications, as these are what enable the financial reporting process and related activities. Any unauthorized access to the financial data stored and processed on computer systems and applications can threaten the company's ability to comply with Sarbox.

Because of the key role that technology plays in storing and enabling access to financial data, and because Section 302 of Sarbanes-Oxley requires the CEO and CFO to personally attest to the accuracy of their company's financial reports, the executive office now essentially mandates that the CIO address the following:

- Enable the CEO and CFO to confidently stand behind the accuracy of data presented in financial reports (Section 302)
- Control and secure access to documents, records, and financial data (Section 404)

Section 103: Auditing, Quality Control, and Independence Standards and Rules

Among the various requirements of Section 103, companies must maintain an audit trail by retaining relevant documents for at least seven years.

Section 302: Corporate Responsibility for Financial Reports

The CEO and CFO must personally certify the accuracy of financial reports.

Section 404: Management Assessment of Internal Controls

Executive officers must implement, assess, and publicly report on the effectiveness of their internal controls for financial reporting.

Section 409: Real Time Issuer Disclosures

Companies must disclose, in real time, any event that may cause a material change in their financial condition.

- Store electronic documents and records for seven years and ensure their integrity (Section 103)
- Audit (log and report) all network access that may impact financial applications and financial data (Section 404)
- Enable real-time reporting of events that could materially impact enterprise profitability (Section 409)

In order to accomplish these Sarbox-related goals, the CIO faces his or her own set of unique challenges. For one, because of the lack of separate budgets for regulatory compliance, security, and other business requirements, the CIO must leverage a single budget to address multiple business needs. In the interest of maximizing efforts and the value of technology investments, the CIO needs to implement a sustainable model that can be applied to other compliance initiatives that dictate privacy and IT controls. Most importantly, the CIO must achieve all this while ensuring that overall business needs are satisfied. In other words, the CIO is tasked with cost-effectively delivering unique business resources to partners, customers, and a distributed workforce, while keeping the company's systems and data secure.

As part of controlling the costs associated with achieving and maintaining compliance, organizations can benefit from automated controls such as identity and access management, which reduce the effort, time and cost associated with audits. In fact, in its *Auditing Internal Control over Financial Reporting, Staff Questions and Answers* issued on May 16, 2005, the PCAOB stated that if general controls over program changes, access to programs, and computer operations are effective and continue to be tested, and if the auditor verifies that the automated application control has not changed since the auditor last tested the application control, the auditor may conclude that the automated application control continues to be effective without repeating the prior year's specific tests. The PCAOB concludes that such a strategy "presents an area of potential audit efficiency for those companies that have made investments in effective Information Technology ("IT") general controls."

IDENTITY AND ACCESS MANAGEMENT'S ROLE IN COMPLYING WITH SARBANES-OXLEY

When it comes to system security and the control of access to systems and applications, Sarbox is not explicitly prescriptive. However, by comparing industry best practices for security and control of other types of information with Sarbox legislation, the following common requirements for internal control become clear:

- Access rights in distributed and networked environments should be effectively controlled and managed.
- Companies should be able to remove terminated employees' or contractors' access to applications, file and data storage, and systems immediately.
- Companies should be able to confirm that only authorized users have access to sensitive information and systems.
- Control over access to multiuser information systems should be implemented — including the elimination of multiple user IDs and accounts for individual persons.
- The allocation of passwords should be formally managed, and password security policies must be enforced.
- Appropriate measures must be taken to prevent unauthorized access to computer system resources and the information held in application systems.

- Periodic assessments and audits of access rights and privileges must be performed.

Essentially, these requirements all touch upon the need to deliver the right information and business processes to the right people, and doing so starts with controlling identity. The decision to grant people access to business resources or data is based on their role with and within the organization, which is managed as “identity information.” Unfortunately, in most organizations, this information is dispersed across multiple systems, requiring IT staff to manually manage identity information and access control—system-by-system, person-by-person. In some cases, administrators must enforce separate user and rights management processes for each application or department, for hundreds or thousands of users. This complex and cumbersome task is both time-consuming and prone to error. And the problems increase as access is extended to customers, business partners, and suppliers. Given this complexity, it is no wonder that many CIOs are turning to identity and access management technology to effectively manage the process of addressing some Sarbox requirements.

Identity and access management provides the ability to manage users and their access to information systems and data. According to Mike Neuenschwander of the Burton Group in an *Enterprise Identity Management Market 2004* report, “identity management is no longer just a good idea—it’s imperative. As enterprise IT departments grapple to reduce risk, thwart attacks, comply with regulations, and instill confidence in customers and partners, the discussion inevitably leads to improving the infrastructure for digital identity.” In fact, organizations can address each of the common requirements for internal control in an efficient, cost-effective manner by applying a comprehensive, enterprise identity and access management solution.

By supporting the following capabilities, identity and access management solutions help enterprises securely and efficiently manage user identities and access to sensitive data and systems, resulting in improved and simplified Sarbox compliance processes:

1. Directory-based user management
2. Business-driven authoritative data sources
3. User provisioning/deprovisioning
4. Password management
5. Password quality enforcement
6. Access management
7. Account management and self-service
8. Identity-driven storage management
9. Secure Web-based portal and dashboard
10. Activity monitoring, auditing, and reporting

As the PCAOB clarified, enterprises can reduce the cost, time, and risks associated with compliance activities by leveraging technology. For sections 103, 302, 404, and 409, identity and access management solutions provide the technical capabilities that underlie sustainable compliance.

NOVELL IDENTITY AND ACCESS MANAGEMENT SOLUTIONS

Novell provides the industry's most innovative and comprehensive portfolio for identity and access management solutions that enable users to gain control of identity and deliver information to the right users wherever they are. This portfolio includes the following products and sub-components that are critical to the success of any identity and access management solution:

Novell® Identity Manager

An automated user-provisioning solution that enables you to streamline user administration, increase security, reduce costs and enhance support for regulatory compliance.

Novell Identity Manager enables enterprises to securely and automatically manage the access needs of the ever-changing user community. The solution enables IT administrators to deliver fast, role-based resource access to new users, synchronize multiple passwords into a single login, and modify or revoke access rights instantly, all of which increases your security and reduces risk.

The solution's self-service features enable users to request resources, manage approval workflow, maintain their own passwords according to business policies, all of which streamlines administration and reduces operating costs. Novell Identity Manager also enables you to create, reuse and share workflows based on industry best practices or regulatory frameworks to speed business process and ensure regulatory compliance.

Novell eDirectory™

Novell eDirectory is the foundation for the world's largest identity management deployments—a high-end directory service that allows businesses to manage identities and security access for employees, customers and partners. More than an LDAP directory, eDirectory is uniquely capable of meeting the demands of large-scale, high-end directory deployments where cross platform compatibility, ease of management, scalability and security are vital requirements. Built on open standards, eDirectory can serve as a secure repository of identity and resource data for both Novell and partner developed security and identity solutions.

“Identity management is no longer just a good idea—it’s imperative. As enterprise IT departments grapple to reduce risk, thwart attacks, comply with regulations, and instill confidence in customers and partners, the discussion inevitably leads to improving the infrastructure for digital identity.”

Mike Neuenschwander

“Enterprise Identity Management Market 2004: IdM Suites Go Mainstream,”
Burton Group, May 26, 2004

Novell iChain®

Novell iChain delivers identity-based Web security services that control access to network resources across technical and organizational boundaries. It provides users with secure authentication and access to portals, Web-based content, and Citrix® Thin Client services. By separating security from individual applications and Web servers, the solution enables centralized, policy-based management of authentication and access privileges for Web-based environments.

Novell BorderManager®

Novell BorderManager is an identity enabled firewall and VPN solution for safeguarding your network while enabling secure access. Grant remote and mobile employees secure, role-based access to systems and data. Protect your network with multi-layered security features like advanced content filtering that shields you from undesirable Internet content that may contain programs that destroy or steal data. BorderManager supports advanced authentication methods including tokens, smart cards, x.509 certificates, biometrics and more.

Novell® SecureLogin

Novell SecureLogin provides users with secure client-based single sign-on access to virtually any application in the network. Moreover, because it is integrated with eDirectory and Novell Modular Authentication Service (NMAS), SecureLogin enables organizations to control access to network resources – based on company policies and user profiles – with a single, secure password or using advanced authentication methods, such as smartcards, tokens, and biometrics.

Sentinel™ 5

Sentinel 5 delivers real-time monitoring and remediation for automated security and compliance. With a single view of security and compliance activities across the enterprise, Sentinel 5 combines the benefits of identity and systems management with real-time compliance monitoring. Sentinel 5 enables customers to streamline a previously labor-intensive and error-prone process, cut costs through automation, and build a more rigorous security and compliance program.

Novell® Storage Manager

Novell Storage Manager is the only hardware and platform agnostic storage solution that enables IT administrators to use automated policies that leverage user identity and role to simplify storage management for both the administrator and the end user. Novell Storage Manager automates previously manual tasks such as quota management, directory renaming, migration, storage triage, retirement and audit. The ability to apply unique user identity to storage management and storage access delivers the type of internal control mandated by Section 103 of the Sarbanes-Oxley Regulations.

Novell access control solutions (iChain, SecureLogin & Border Manager) link with Novell application integration and identity-driven, role-based portal solutions enabled by Novell Identity Manager and Sentinel 5. Which makes it possible for enterprises to aggregate data across product lines, business units, and geographies and present it in a clear, concise view of security and compliance that facilitates decision making.

By providing the right key performance indicators to the right managers in real time, executive portals (or dashboards) allow executives to disclose information in near real time to satisfy regulatory requirements.

Novell identity and access management solutions support Sarbox compliance in the following areas:

	Identity Manager	eDirectory	iChain	Border Manager	Secure Login	Sentinel 5	Novell Storage Manager
Centralized User Management	X	X	X				X
Business-driven authoritative data sources	X					X	
User provisioning/deprovisioning	X	X					X
Password Management	X	X	X		X		
Password Quality Enforcement	X	X	X		X		
Access Management	X	X	X	X			
Account Management/ Self service	X				X		
Identity-based storage management							X
Dashboard Reporting & Healthcheck						X	
Activity monitoring, auditing, and reporting						X	

APPLYING NOVELL SECURITY & IDENTITY SOLUTIONS TO SARBANES-OXLEY

According to Robert D. Hugel with Ventana Research in a January 2005 issue of *Intelligent Enterprise Magazine*, “The need to adapt to the more formal control environment of SOX gives companies an opportunity to make their IT systems more useful. Not only can they address the efficiency issues created by 404, but they can also enhance the effectiveness of the finance organization and the entire company.” Like all business initiatives, implementing IT controls for Sarbox compliance revolves around a lifecycle of activities that includes adopting and enforcing policies, controls, and procedures. To satisfy current and future requirements for regulatory compliance, the CIO is best served by following a standard process for addressing each requirement, as outlined below:

- Establish policies

- Identify risks of policies being circumvented
- Develop controls to mitigate risks
- Establish procedures to support the controls
- Implement technology and other elements to carry out the procedures

Following are examples of policies that an enterprise can adopt to meet the requirements of **authorizing** access to, and **recording** and **reporting** on, financial data. As part of establishing these policies, the organization will likely need to develop controls that help mitigate the risks to maintaining and enforcing these policies. Novell identity and access management solutions can be used to implement the procedures necessary to enforce these controls.

"The need to adapt to the more formal control environment of SOX gives companies an opportunity to make their IT systems more useful. Not only can they address the efficiency issues created by 404, but they can also enhance the effectiveness of the finance organization and the entire company."

Robert D. Hugel
*"The Silver Lining in SOX",
Intelligent Enterprise Magazine,
January 2005 issue Volume 8 No.
1, Ventana Research*

Building a Compliance Mindset
Focus on risks. Evaluating risks is critical to writing effective controls and achieving compliance. Remember, controls mitigate risks.

Simplify and consolidate controls. Each process does not require a separate control. A single well-designed control can apply to a number of similar processes.

Look forward to real benefits. Sarbox provides the opportunity to streamline business processes, establish accountability, and **achieve greater agility.**

Policy: Only authorized people can access core financial systems	
Risk: Unauthorized people (either through malicious intent or ignorance) access core financial systems and alter financial data so that it misrepresents the company's financial situation.	
Control: Develop policies that specify who can access certain systems and implement technology capable of executing rules that support the policy.	<p>Procedure: Manage users and rights</p> <p>Enabling Capability and Technology: Novell Identity Manager and Novell eDirectory</p> <p>Novell Identity Manager and Novell eDirectory link all instances of an identity across the dozens of systems deployed throughout the enterprise. Updates based on established business rules are propagated throughout these systems when a change is made in an authoritative source. With Identity Manager, organizations can easily create and manage identities for a variety of constituents based on their roles and rules associated with those roles. This helps ensure that only authorized users have access to sensitive financial data and the systems on which this data is stored and processed. By automating and streamlining identity management-related activities, Novell Identity Manager and Novell eDirectory ease the burden of managing users and rights, while helping to eliminate manual errors that may jeopardize compliance with Sarbox.</p>
	<p>Procedure: Provisioning and De-provisioning</p> <p>Enabling Capability and Technology: Novell Identity Manager</p> <p>The ability to automatically grant and revoke access rights helps meet regulatory requirements, while streamlining administrative tasks. With Novell Identity Manager, organizations can automatically grant new hires immediate access to all the information and resources they need to be productive. The solution links all relevant systems and applications, and automatically creates all necessary user accounts when a new employee is entered into an authoritative source, basing content and resource access privileges on the employee's role. And to facilitate security, Identity Manager automatically and immediately revokes all access privileges once an employee or contractor's relationship with the company is terminated.</p>

Procedure: Access control

Enabling Capability and Technology: Novell iChain, Novell eDirectory, and Novell BorderManager

Novell identity and access management solutions unify and simplify security management by linking all applications, databases, and directories, and allowing organizations to centrally store and manage security rules across those systems. Administrators only need to create security and access rules once, and these rules are then automatically applied to all systems. This not only eliminates the time and expense of creating and maintaining separate security rules on dozens of systems, but also eliminates a major source of administrator errors that could result in security holes.

With Novell iChain, enterprises can control user access to Web environments and enable single sign-on to nearly all Web-based applications and content. Novell eDirectory provides administrators with real-time control over users' access to network resources, enabling instant termination of network access. And to grant remote and mobile employees secure, role-based access to only those systems they are entitled to use, administrators can use BorderManager.

Procedure: Password management

Enabling Capability and Technology: Novell Identity Manager, Novell iChain, Novell SecureLogin, Novell eDirectory

Novell password management solutions offer multiple ways to simplify the management and use of passwords according to business needs. Through password synchronization and/or single sign-on, organizations can reduce the number of passwords that internal and external users need to access corporate systems and information. Fewer passwords lessen the likelihood that users will create easy-to-decipher passwords, and reduce the administrative burden of managing and supporting passwords. Administrators can centrally manage all passwords based on organizational policies, and Novell solutions also allow users to securely reset passwords

	<p>without administrative intervention. Support for advanced authentication features – such as tokens, smart cards and biometrics – further enhance security measures.</p>
	<p>Procedure: Multi-factor authentication</p> <p>Enabling Capability and Technology: Novell Modular Authentication Service (NMAS), a component of Novell eDirectory</p> <p>NMAS is a versatile authentication management solution that provides multi-factor authentication and graded Authentication to Novell eDirectory. Using this component of eDirectory, organizations can combine any number of password, token, X.509 certificate, and biometric login methods to limit access to any data, application, or user on the network.</p>
<p>Control: Ensure auditability of internal control procedures.</p>	<p>Procedure: Logging and reporting on identity management and system events/occurrences</p> <p>Enabling Capability and Technology: Sentinel 5</p> <p>Sentinel 5™ helps organizations audit network activities to ensure that systems are being administered and utilized as intended. This in turn assists in determining and demonstrating how well the organization is complying with external regulations, such as Sarbox. The solution tracks all network events across the network, scrutinizing events on all relevant business applications, assets and for all users. Sentinel 5 monitors for known threats and tracks out-of-policy events that warrant further review. By recording all event data in a single system using a common data structure, delivering real-time event information for notification and monitoring purposes, and providing reporting tools. Sentinel 5 helps organizations investigate and address security information event monitoring for enhanced compliance.</p>
	<p>Procedure: Workflow and approval processes</p> <p>Enabling Capability and Technology: Novell Identity Manager</p> <p>In most organizations, users need approval from one or more individuals before being granted access to systems or services. Novell Identity Manager helps organizations keep the approval process flowing quickly, automatically, and cost-effectively by</p>

	<p>automatically passing documents, information, or tasks from one participant to another for action, according to a set of procedural rules. It supports email notification of workflow status and action requirements, and includes a user interface that makes it easy to administer the workflow.</p>
<p>Policy: Maintain audit work papers and other information related to all audit reports for a minimum of seven years.</p>	
<p>Risk: The company fails an audit because documents are lost and/or the integrity of the documents cannot be guaranteed due to lack of change control and access records.</p>	
<p>Control: Establish a document storage system that incorporates identity management and audit capabilities.</p>	<p>Procedure: Identity-controlled file storage</p> <p>Enabling Capability and Technology: Novell Storage Manager</p> <p>Novell Storage Manager is an event-driven file-system management solution that incorporates identity management to serve as an effective evidence-based repository for Sarbox section 103 requirements. Novell Storage Manager enables policy-based lifecycle provisioning and de-provisioning of personal and group storage, simplifying access and management of storage based on users' identities. Whenever user and group accounts are created, moved, or deleted in an authoritative system, Novell Storage Manager automatically creates, moves, or deletes disk storage. This ensures that as users migrate to different parts of the organization, their data automatically follows them. And as users leave the network, Novell Storage Manager can either delete their stored data immediately or defer deletion for a specified time period.</p>
<p>Policy: Management must disclose, in real time, any event that causes a material change in the company's financial condition.</p>	
<p>Risk: Lack of integration among disparate systems make it impossible to deliver the right information to the right people in a timely manner.</p>	
<p>Control: Develop the capability to identify and deliver information to the appropriate executives as events occur.</p>	<p>Procedure: Integrate Security and Identity information into one view of security and compliance</p> <p>Enabling Capability and Technology: Sentinel 5</p> <p>Using Sentinel 5 organizations can deliver regulation and role-specific reports for continual assessment and attestation of compliance based unified, real-time view of all security and compliance events across the network. These reports also support and deliver drill down analysis and modeling for "what if</p>

	<p>scenarios" and proactive management needed for comprehensive and proactive security and compliance management. Sentinel 5 can be pre-configured to gather data from any enterprise system, process or device that is relevant to the specific regulatory framework (in this case Sarbanes-Oxley).</p>
	<p>Procedure: Create role-based, Compliance dashboards</p> <p>Enabling Capability and Technology: Seninel 5, Novell Identity Manager, and Novell iChain</p> <p>To address the need for access security and compliance monitoring information in an actionable manner, many enterprises are turning to 'executive dashboards" as a means to deliver real time health-checks on an entire enterprise's current compliance and security position. Building upon Novell services-based enterprise message bus architecture, Sentinel 5 gathers information from existing data sources and business intelligence tools, and presents it in real-time to the right people. Novell iChain can be used to provide users with secure authentication and access to this dashboard from outside the firewall, to further ensure constant access to information without sacrificing security.</p>

ACHIEVING SUSTAINABLE COMPLIANCE AS A COMPETITIVE ADVANTAGE

While many business leaders are daunted by the requirements of complying with the Sarbanes-Oxley Act, forward-thinking executives will view Sarbox as an opportunity to develop and implement processes that improve overall business practices. Implementing a standard process to achieve Sarbox-related goals offers a strategic approach that enables *sustainable compliance* and helps streamline compliance efforts and reduce compliance-related costs.

A solid security event monitoring and access control infrastructure makes it easier to establish necessary controls by offering automated systems that provide the security and audit trails that help ensure long-term compliance. But Sarbanes-Oxley compliance is only one of many business challenges and organizations need a framework that helps them address compliance efforts beyond Sarbox, along with other strategic initiatives.

Security and identity solutions from Novell provide such a foundation with the flexibility and scalability to address IT controls and a variety of business issues, such as security, productivity, and additional compliance regulations that mandate controlling access to corporate information. In fact, “many control activities - such as deploying firewalls, access controls and audit logs - represent [SOX compliance] best practices you should be following anyway,” says Daniel Blum of Network World in a May 2005 article entitled *Risk management, Controls key to SOX*

With security and identity solutions from Novell, organizations can safeguard systems and deliver the right resources to the right people—securely, efficiently, and cost-effectively by:

- Replacing time and resource intensive reconciliation and reporting with automated solution.
- Integrated systems eliminate the need for duplicative threat management and compliance point solutions.
- Ability to deliver regulation-specific “tone at the top” security and compliance reporting for the entire enterprise can shorten length and depth of audit cycles.

“While SOX compliance is expensive, much of the effort is reusable. Every company should be doing risk management, for example. Many control activities - such as deploying firewalls, access controls and audit logs - represent best practices you should be following anyway.”

Daniel Blum

Risk management, Controls key to SOX Network World, May 2, 2005

- Real-time event correlation and response means costly security breaches can be avoided.
- Automatically provisioning new users with access to business resources based on their role, increasing productivity for users and administrators.
- Automatically modifying or rescinding access the moment a user's role changes or ends to keep confidential resources safe.
- Automatically provisioning and de-provisioning personal and group storage, simplifying access to and management of documents stored, based on users' identities.
- Implementing secure password management to mitigate security risks, minimize associated costs, and improve the user experience.
- Providing secure, remote access from any location to resources based on a user's role or relationship with the organization.
- Maintaining an audit trail that demonstrates compliance with internal business policies and external regulations to minimize liability and risk.

Enterprises can take advantage of consulting and implementation support and services offered by Novell and its systems integrators and global professional services partners to ensure the successful implementation of a solution that helps the organization gain control of identity. In addition, Novell and its partners are ready to collaborate with any organization's established Sarbox professional services consulting partners to lay the foundation for other identity-driven business initiatives that enable the agile enterprise.

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

1 888 321 4272 U.S./Canada
1 801 861 4272 Worldwide
1 801 861 8473 Facsimile

Novell, Inc.
404 Wyman Street
Waltham, MA 02451 USA

www.novell.com