

A large, abstract graphic on the left side of the page, consisting of several overlapping, curved, semi-transparent shapes in shades of gray, creating a sense of depth and movement.

# THE CONVERGENCE OF **PROVISIONING AND IDENTITY AUDITING**

The Key to Cost-Effective Compliance and Collaboration  
White Paper  
February 2008

## Table of Contents

<b>Executive Summary</b> .....	<b>3</b>
<b>Identifying the Drivers for the Convergence of Provisioning and Identity Auditing</b> .....	<b>4</b>
The Risk of Non-Compliance .....	4
The High Cost of Compliance .....	4
The Inability to Collaborate and Scale Infinitely .....	5
<b>Identifying the Opportunities Associated with Convergence</b> .....	<b>6</b>
Addressing Fundamental Compliance Issues .....	6
Controlling the Costs of Compliance .....	7
Achieving Scalability and Interoperability to Support Growth .....	7
<b>Using Sun’s Converged Capabilities to Meet Major Business Objectives</b> .....	<b>8</b>
<b>Solution Scenarios: Real-World Converged Provisioning and Identity Auditing</b> .....	<b>9</b>
Scenario 1: Ensuring Segregation of Duties at a Large Manufacturing Company .....	9
Scenario 2: Automating Access Review at a Major Insurance Company .....	9
Scenario 3: Protecting Employee Privacy at a Global Technology Company .....	10
<b>Conclusion</b> .....	<b>11</b>

## Chapter 1

# Executive Summary

When identity management began to come to the forefront of information technology in the early 2000s, businesses and other organizations faced a completely different set of identity-related challenges than they do today. At that time, the economy was struggling and the most important business drivers for identity management were the needs to increase productivity and lower costs.

Today, high productivity and low cost continue to be concerns, but they have been joined by two relatively new phenomena: an array of regulations governing data integrity and privacy and the emergence of the Internet as a major channel for commerce. The first has moved the auditing capabilities of identity management to the forefront of the IT infrastructure. The second has created a demand for companies to collaborate online with more third parties than ever before — a demand that identity management can help fulfill. Finally, this level of collaboration requires the ability to scale to accommodate more connected users, which the right identity management solution should be able to do.

The merging of cost, compliance, and online commerce as chief business concerns is driving the convergence of provisioning and identity auditing capabilities as well as the demand that such a converged solution be both sustainable and highly scalable. This paper will:

- Examine today's business drivers for the convergence of provisioning and identity auditing
- Consider the business opportunities associated with a converged approach
- Describe the converged provisioning and identity auditing capabilities of Sun Java™ System Identity Manager
- Explore scenarios that demonstrate how Sun's converged solution makes it possible to meet today's key business objectives

## Chapter 2

# Identifying the Drivers for the Convergence of Provisioning and Identity Auditing

## The Risk of Non-Compliance

In the early days of identity management, compliance was not the business priority that it has become today. There may have been a few industries — banking, insurance, and utilities perhaps most prominently — that were more highly regulated than others. But there was hardly the focus on regulatory requirements that there is now. Since 1996, lawmakers have responded to corporate financial scandals and to the rise of identity theft by passing a great deal of new legislation governing data integrity and privacy. Here are just a few examples:

- **The Sarbanes-Oxley Act of 2002** has become perhaps the best-known, most important, and often most-feared regulation in the United States. Sarbanes-Oxley requires all public companies in the U.S. to protect the integrity of financial data in a number of very specific ways including, for example, avoiding the erroneous aggregation of a user's access privileges to certain types of data. It also carries the threat of stiff penalties for non-compliance with its provisions, including prison time — not only for those who violate its provisions, but also for the executives in charge when violations occur.
- **The Health Insurance Portability and Accountability Act (HIPAA)** affects the entire healthcare industry in the United States. Non-compliance with the privacy-related portion of this regulation can result in criminal penalties of as much as \$250,000 and up to ten years in prison, depending on the severity of the violation.
- **The Gramm-Leach-Bliley Act** requires that financial institutions ensure the security and confidentiality of customers' personal information against internal and external threats. As with Sarbanes-Oxley and HIPAA, this requirement applies equally to information online and on paper.
- **State-level legislation** has also been widespread in the last few years. This is important because the effects of state regulations can extend beyond the state in which they were passed. A recent California law requiring companies to protect their customers' private information covers their customers in other states. For an online business, that could be every state in the country.

To help companies comply with these laws, a comprehensive identity management solution should provide 1) capabilities for detecting and remediating any access policy violation that could put the company in violation of a regulation and 2) capabilities for preventing violations from occurring in the first place.

## The High Cost of Compliance

One of the most daunting aspects of compliance is the cost associated with it. Complying with regulations and passing regulation-driven audits has become increasingly critical — and costly. Everyone from business writers to consultants has been sounding a cry of alarm about this for quite some time:

- Back in 2004, CIO magazine predicted that as the number of regulations increased, so would the cost of compliance. Almost any business that has to comply with multiple regulations today would have to agree that the prediction has come true.

- More recently, *BusinessWeek online* reported that “even though a lot of good has come from the new corporate regulation ushered in by the likes of Enron and WorldCom, cleaning up has come at a cost. And, for public companies today, that cost doesn’t seem to be declining with time.”
- PricewaterhouseCoopers laments the cost of compliance and asks, “How long can companies continue with the ‘compliance at any cost’ approach?”

Just why is the cost of compliance so high? One reason is that since compliance has only recently become an important part of the operations of many companies, they have not been prepared to approach it in a cost-efficient manner. The processes many companies use to meet audit requirements are likely manual ones, often requiring the exchange of a flurry of emails and other communications between auditors and company officials. This involves an enormous amount of work, which takes a lot of time and involves many people — and that makes it expensive.

The same companies that currently automate activities ranging from user provisioning to supply chain management are realizing that they need to do the same with compliance. Through automation, they can make their audit- and compliance-related processes significantly more efficient and less costly.

### **The Inability to Collaborate and Scale Infinitely**

The online store was just beginning to have a major presence in business in the early 2000s. Today, it has overwhelmingly changed the way people acquire products and services — and the way businesses provide them. The rise of service provider collaborations is a good example. Companies such as communications service providers, who must constantly find new ways to satisfy customers’ growing demand for more products and services, are increasingly collaborating with other service providers to meet that demand.

That’s when a company’s extranet becomes its intranet. As a company collaborates with other entities online, the processes for granting and changing access to resources and for ensuring the security of that access must extend beyond traditional enterprise boundaries. Online commerce is just one aspect of this phenomenon; consider also the online relationships maintained by companies with its outsourcers, such as benefits administrators. These relationships also depend on being able to collaborate freely yet securely online.

Along with the need for collaboration comes the need for scalability. When a company collaborates online with other companies, it must accommodate more users who require access to its systems and resources online. It’s not unusual today for a company’s relationships with other companies to result in environments of millions of users. And that means that processes such as provisioning, as well as policies surrounding secure access, must apply not just to employees inside the company, but also to users in all the other companies with which it maintains relationships. Identity management is central to executing these processes and applying these policies. The problem is that many of today’s identity management solutions are generally not designed to scale to the extent that online collaboration requires.

## Chapter 3

## Identifying the Opportunities Associated with Convergence

A highly scalable identity management solution that combines provisioning and identity auditing can be a powerful force for enabling improved compliance at a lower cost. A converged solution makes it possible to set a baseline for compliance and maintain that baseline by using identity auditing to detect violations. In addition, because the provisioning process is intrinsically linked to the compliance process, a converged solution also makes it possible to consolidate centralized provisioning with compliance checking, thus enabling prevention and not just detection.

### Addressing Fundamental Compliance Issues

Handling provisioning and identity auditing separately made sense in the days when compliance was not a major initiative for most businesses. But now that these issues have become so important, addressing them together makes more sense because together, provisioning and identity auditing can provide complete capabilities to both detect and prevent compliance violations.

An automated converged solution makes it possible to detect and remediate existing policy violations in one smooth process, as well as to prevent potential violations from ever occurring. Without a converged solution, detecting violations can take weeks at the end of the quarter — and all of the remediation activity is manual and therefore painfully slow. By contrast, when the automated identity auditing component of a converged solution detects a problem, that information can be relayed to the provisioning component, which can then automatically remediate it. For example, identity auditing can detect if a user who recently moved into a new role in the company retained his or her access privileges to resources associated with the old role, which would be a violation. Then, provisioning can instantly and automatically revoke the inappropriate access. This process is demonstrated in the simple illustration that follows.

- When a user changes jobs within a company, identity auditing can detect whether a segregation of duties violation will occur as a result and automatically alert provisioning before the violation occurs.

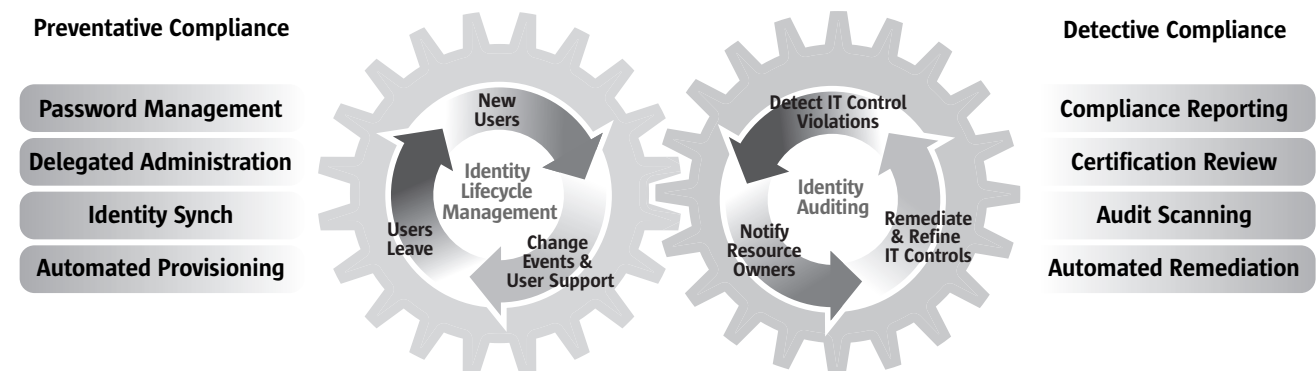


Figure 1. Converged provisioning and identity auditing reduces the risk of non-compliance by creating a continuous audit cycle, which makes it possible to detect and prevent compliance violations in an ongoing, sustainable manner.

Being able to link auditing to provisioning is essential to complying with, for example, Sarbanes-Oxley rules regarding segregation of duties or erroneous aggregation of privileges. That's because when separate manual processes are used for auditing, it can take a considerable amount of time to detect a problem, during which the company may technically be in violation of the law. Furthermore, once a problem is detected, the existence of separate systems requires a manual effort to ensure that provisioning resolves the issue.

In addition, identity scanning for access privileges can provide the benefit of always being able to know what resources a user has access to and not just what resources that user should have access to. By continuously scanning and reconciling what systems and facilities a user can access, companies can maintain a better baseline and have fewer violations.

### **Controlling the Costs of Compliance**

Many companies recognized long ago that automating the provisioning aspect of identity management would reduce costs, since an automated solution speeds provisioning processes and eliminates costly manual errors. A converged provisioning and auditing solution specifically reduces compliance costs by also automating identity auditing, which many companies still handle manually, and by automatically synchronizing provisioning and identity auditing information so that each always has current, complete insight into the other.

While automated compliance processes could contribute significantly to reducing the costs of compliance, the troubling fact is that automation is not widely implemented today. "The Executive View of Compliance," a report jointly published by Sun and PricewaterhouseCoopers in 2005, reviewed the results of a Forrester Research study investigating executive responses to compliance demands. One of the key findings was that the vast majority of companies — 77 percent — were putting manual processes and procedures for compliance in place. Making the transition to automated solutions is critical to controlling the cost and effort of ongoing compliance.

A converged solution also achieves lower costs by eliminating the unnecessary duplication of effort associated with having two separate mechanisms for provisioning and identity auditing. Instead of using two IT teams to address these two issues, companies can streamline to one group with responsibility for both. The other team can then be redirected to more productive activities.

The automation of periodic access review is an excellent example of how an automated, converged solution can eliminate unnecessary effort. A converged solution can automate the collaboration and data exchange between provisioning and identity auditing that is usually done manually. This saves significant time and trouble. Another advantage is that as the implementation matures over time, a company no longer has to review all users' access every time — only those whose roles have been changed by provisioning. This further streamlines the access review process.

### **Achieving Scalability and Interoperability to Support Growth**

A converged provisioning and identity auditing solution that is designed for maximum scalability and interoperability will address compliance challenges and, at the same time, enable the large-scale collaboration that fosters healthy growth and a competitive edge in today's online commerce environments. The challenge is finding a single vendor that can provide a single, scalable solution that combines provisioning and identity auditing. The alternative is to continue to implement multiple solutions piecemeal, which can easily result in integration issues that are both costly and time-consuming.

## Chapter 4

# Using Sun's Converged Capabilities to Meet Major Business Objectives

Sun Java™ System Identity Manager is the first converged solution for provisioning and identity auditing in the identity management space. Its capabilities specifically enable companies to meet three major business objectives: compliance, cost control, and collaboration.

- **Complete Identity Lifecycle Management Tied to Auditing for Violations**  
Identity Manager uses policy-based provisioning and workflow to prevent compliance violations during identity administration. Policy-based provisioning and workflow enable complete, automated identity lifecycle management in which potential violations are flagged before the system grants entitlement to resources.
- **Automated Early Warnings About Policy Violations**  
The identity audit scanning capability of Identity Manager reduces the risk of non-compliance by continuously checking for violations in identity data in target applications and automatically detecting policy violations.
- **Streamlined, Ongoing Review of User Access with Instant Remediation**  
Administrators can use the automated entitlement review capability to schedule regular reviews of access privileges and policy violations. If violations are found, Identity Manager automatically initiates remediation. This streamlines and automates the ongoing access privilege review process, reducing the cost and time associated with compliance.
- **Complete Visibility into Current Compliance Exposures**  
Identity Manager's compliance dashboard displays a summary view of compliance metrics at all times and also displays violations, exceptions, and anomalies. Executives have complete visibility into security and compliance exposures at any given time to help with decision-making.
- **Comprehensive Compliance Reporting**  
Preconfigured reports for commonly required identity audit data are included with Identity Manager. In addition, the solution reports on policy violations, remediations, and exceptions and enables custom reports of audit data.
- **Scalable Provisioning and Identity Auditing for Extranet-Facing Environments**  
With Identity Manager, companies have a scalable option in extranet-facing applications and portals. The solution's extranet and federated identity administration capabilities can help introduce more new applications and services to customers quickly — without compromising security or compliance controls. The solution has been tested in environments with millions of users.

## Chapter 5

# Solution Scenarios: Real-World Converged Provisioning and Identity Auditing

The following scenarios provide typical examples of specific provisioning and identity auditing-related challenges that can be addressed by the converged capabilities of Identity Manager.

### Scenario 1: Ensuring Segregation of Duties at a Large Manufacturing Company

**Situation:** Maria, an accountant working in accounts receivable, takes the opportunity to move to another group within the company, where she will work in accounts payable. When she starts her new job, she is quickly provisioned with access to the appropriate network resources to fulfill her new responsibilities. Meanwhile, she continues to have access to resources that were tied to her old position. This puts the company in violation of the segregation of duties requirements of Sarbanes-Oxley, under which it is a conflict of interest to have access to both the A/R and A/P systems. The violation goes unnoticed until a Sarbanes-Oxley auditor asks Maria's former manager in A/R to confirm users' access privileges, and the manager indicates that Maria left the department some time ago.

**Problem:** Because provisioning is automated but auditing is not, Maria ends up having access to two sets of systems and resources, creating a potential risk to the integrity of financial data at the company. Even if she never again accesses the systems associated with her old job, the potential for her to do so would continue to pose a threat. Worse yet, this potential is ultimately uncovered by a Sarbanes-Oxley auditor doing a routine review of access — putting the company at risk for failing the audit and being charged with violating Sarbanes-Oxley requirements for segregation of duties.

**Solution:** The company adopts Identity Manager, which automates provisioning and identity auditing within one solution. Because the two capabilities are linked, an employee who leaves one area to join another can be provisioned for new responsibilities instantly — and, at the same time, automatically deprovisioned for resources associated with the previous position. This eliminates the risk of violating Sarbanes-Oxley requirements requiring segregation of duties and prohibiting erroneous aggregation of privileges.

### Scenario 2: Automating Access Review at a Major Insurance Company

**Situation:** The company has 500 different applications that are all critical to its business, and 80% of employees need to have role-appropriate access to these applications. These employees' roles are constantly shifting due to promotions, transfers, or other changes, and their access privileges must change accordingly.

**Problem:** Managers and auditors have to certify that each user's access to applications is appropriate. This is done manually by generating reports and sending them to users' managers and application owners to review and sign off on them. Because of the number of applications, the constant change in roles, and the sometimes less-than-timely response by reviewers, the process can take an entire year. During that time, the company is at risk because compliance violations are going undetected for so long.

**Solution:** The company can accelerate the access review process by implementing Identity Manager to automatically track approvals, notify managers when it's time for a review, and escalate when reviewers fail to respond. Identity Manager also generates reports that capture all approvals and document all remediations for auditing purposes. By automating processes in order to dramatically streamline access review, Identity Manager can make compliance far less costly and time-consuming for this company.

### **Scenario 3: Protecting Employee Privacy at a Global Technology Company**

**Situation:** Charles leaves his position in the human resources department as liaison to the company's benefits administrator, and takes a job in the company's marketing department. Even though it's no longer appropriate for him to have access to the private health insurance data that was available to him when he worked in HR, he continues to have access to it until someone in IT preparing for an audit notices the problem. Even then, it's still another few days before someone handling provisioning is advised of the situation and deprovisions Charles. Meanwhile, Charles has been entertaining his new colleagues in marketing by sharing their manager's health insurance records with them.

**Problem:** Charles' actions violate not only the employee privacy policies of the company, but also the privacy provisions of HIPAA, the regulation that governs all environments in which people have access to individuals' personally identifying healthcare information. Charles' actions could result in the company being fined for its HIPAA violations.

**Solution:** In addition to dismissing Charles, the company implements Identity Manager. The solution's converged provisioning and identity auditing capabilities enable much tighter controls over access to private employee data. The next time someone leaves the benefits area of HR to join another department, action to strip that person of access to healthcare-related employee records will be initiated automatically the moment the change occurs.

## Chapter 6

# Conclusion

Identity management provisioning and identity auditing capabilities are central to helping companies achieve regulatory compliance at a reasonable cost. In this quest, it is no longer enough to automate provisioning processes while continuing to try to meet auditing requirements manually. Only a converged provisioning and identity auditing solution can provide the combined capabilities, streamlined operations, and scalability that companies need to be compliant, control costs, and stay competitive.

To learn more about Sun's converged approach to provisioning and identity auditing, visit [www.sun.com/identity](http://www.sun.com/identity).

