

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.

ROLE MANAGEMENT: THE KEY TO COST-EFFECTIVE COMPLIANCE AND PROVISIONING

White Paper
May 2008

Table of Contents

Executive Summary	1
Identifying the Drivers for Role Management	3
Security and compliance	3
The high cost of compliance	4
The need for automated provisioning	5
Identifying the Opportunities Associated with Convergence	6
Addressing fundamental compliance issues	6
Controlling the costs of compliance	7
Further automating the provisioning process	8
Using Sun’s Integrated Role Management Solution to Meet Major Business Objectives	9
Solution Scenarios: Real-World Role Management	10
Scenario 1: Ensuring segregation of duties at a large manufacturing company	10
Scenario 2: Automating recertification at a major insurance company	11
Scenario 3: Protecting employee privacy at a global technology company	11
Conclusion	13

Chapter 1

Executive Summary

Identity and access management (IAM) continues to pervade IT initiatives across the enterprise. The needs of companies to conduct business on a global scale will only continue to increase, regulatory requirements aren't getting any easier to comply with, and organizations must continue to look for efficiencies and drive down costs wherever possible to remain competitive. In this environment, IAM solutions must continue to be innovative and meet the growing and changing needs of the enterprise.

The drivers for an IAM solution are still the same: reduce costs, increase productivity, comply with regulatory requirements, and ensure users have appropriate access to critical data, systems, and applications. However, the maturation of IAM solutions and their use in production deployments have given rise to two new drivers: role management and entitlements management. The natural evolution of any user provisioning solution will result in some type of role management solution, better enabling the enterprise to manage the entitlements associated with those roles. However, even with a role management solution, the traditional IAM drivers still exist; therefore, role management becomes a critical component of a robust IAM solution.

What exactly is role management, and how does it address the aforementioned drivers? Role management allows access to be granted based on job title and function. For example, John is a new employee working in accounts receivable at Company X. John needs access to the following resources to do his job: email, Oracle Financials, and the accounts receivable database. Without a role management solution, John would have to be granted access to the raw IT entitlements associated with each of these resources (Microsoft Exchange Server 2007, IBM DB2, and so on). These entitlements have little if any meaning to John's manager, who must ultimately approve his access. A role management solution greatly simplifies the approval process for John's manager. Instead of approving a raw list of IT entitlements, John's manager simply needs to approve that John has been assigned the correct job title or business roles, for which the appropriate entitlements have already been assigned. A role management solution effectively connects the business to IT by enabling provisioning and auditing using meaningful business terms rather than cryptic descriptions of fine-grained IT entitlements.

The continuing needs of organizations to increase efficiencies, drive down costs, comply with regulatory requirements, and ensure appropriate access from within and outside of the enterprise are the primary drivers for a robust IAM solution, of which role management is a vital piece. This paper will:

Examine today's business drivers for a role management solution

- Consider the business opportunities associated with a role management solution
- Describe the role management capabilities of Sun™ Identity Manager software and its integration with Sun™ Role Manager software
- Explore scenarios that demonstrate how Sun's integrated solution makes it possible to meet today's key business objectives

Chapter 2

Identifying the Drivers for Role Management

Security and compliance

Regulatory compliance is a mandatory, and often costly, requirement of operating in today's business environment. Noncompliance can not only result in significant financial loss and brand erosion, it can also result in actual jail time for CFOs and CISOs. Corruption and scandal at some of the largest public companies have given rise to stricter regulations and closer scrutiny by regulatory bodies. 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 U.S. public companies to protect the integrity of financial data in a number of very specific ways, including avoiding the erroneous aggregation of a user's access privileges to certain types of data. It also carries the threat of stiff penalties for noncompliance 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. Noncompliance with the privacy-related portion of this regulation can result in criminal penalties of as much as \$250,000 and up to 10 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:

- Detect and remediate any access policy violation that could put the company in violation of a regulation
- Prevent violations from occurring in the first place
- Allow provisioning and auditing to be performed using the language of the **business** — not the language of IT.

The high cost of compliance

One of the most daunting aspects of compliance is its associated cost. As regulators and auditors become more savvy and sophisticated, compliance becomes that much more costly and difficult. Media and industry professionals have warned of increasing compliance costs for years:

- 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.
- *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.”

Why is the cost of compliance so high? Tighter regulations, closer scrutiny by regulators and auditors, and the increasing need for opening access to partners and customers are some of the primary culprits. In addition, outsourcing and globalization have resulted in an increased need to open up the enterprise to partners and customers. With openness comes risk, and the need for robust safeguards that not only secure the enterprise’s critical data and applications, but also ensure regulatory compliance in terms of accessing that data. In this environment, compliance is very costly, especially if any aspect of it is being done manually. These costs only become exacerbated in larger organizations.

Costs can be mitigated and reduced with a robust IAM and role management solution. Enforcing audit policy at the time of provisioning ensures users have access to only those applications and resources needed to do their jobs. Automating the audit process and remediating violations using predefined workflows help to drastically reduce auditing costs. Provisioning and auditing at the business role level adds significant efficiencies and a drastically increased level of control when managing users’ access to critical resources and applications across the enterprise.

The need for automated provisioning

As organizations grow and become more global, provisioning users across the enterprise becomes an increasingly daunting task. Decentralized provisioning is not only inefficient and costly, it also increases the risk of audit policy and regulatory violations. Decentralized provisioning is prone to human error, lacks an audit trail, and increases the risk of abuse and malfeasance by disgruntled or malicious employees. Risk is also introduced when employees change jobs and access isn't appropriately adjusted or removed. Failing to appropriately adjust or remove users' access when job changes occur can result in superuser-access and segregation-of-duties (SOD) violations.

Automated provisioning effectively eliminates many of these risks, especially when combined with auditing and role management capabilities. Provisioning users to critical resources and applications in an automated fashion from a single platform provides several significant benefits. Automated provisioning allows centralized control of resources and applications that have historically existed in silos. This provides a much greater level of control over access to those resources. Checking audit policy at the time of provisioning ensures regulatory compliance, thus preventing audit policy violations. Provisioning using workflows that model existing business processes helps to automate the approval process associated with granting access to particular resources.

All these benefits are even further enhanced through integration with a robust role management solution. Provisioning at the business role level adds another level of automation, further increasing productivity and reducing costs associated with provisioning and auditing. Role management also greatly reduces the risk of managers inadvertently creating SOD violations by granting carte blanche access to their direct reports. Business roles allow entitlements to be described in a way that is meaningful to non-IT users. It's all too easy for a manager to approve a raw list of cryptic IT entitlements that have little or no business meaning in the context of an employee's actual job function. With a role management solution, managers can instead approve roles that have a meaningful business context.

Chapter 3

Identifying the Opportunities Associated with Convergence

A highly scalable identity management solution that combines provisioning, identity auditing, and role management 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, enabling prevention and not just detection. Role management provides the additional layer necessary to further streamline the provisioning and auditing processes, enabling increased efficiencies and greater controls over users' access.

Addressing fundamental compliance issues

A role management solution provides the tools necessary to enable greater control over compliance with regulatory requirements. The migration from decentralized provisioning to centralized, automated provisioning solutions introduced greater efficiencies and enabled greater control over users' access. Combining provisioning and auditing added an additional level of efficiency and control by creating the ability to do compliant provisioning. Compliant provisioning allowed audit policy violations to be found at the time of provisioning instead of as the result of a costly audit. The natural evolution of this combined approach has inevitably led to the addition of a role management component, providing even greater controls over granting access and ensuring compliance. Integration with role management also begins to involve the business in ensuring access compliance by representing users' entitlements in a meaningful business context.

Linking provisioning and auditing at the business role level is essential to complying with, for example, Sarbanes-Oxley rules regarding SOD or erroneous aggregation of privileges. Using disparate and manual processes for auditing at the individual user level can take a considerable amount of time to detect a violation, during which the company may technically be breaking the law. In addition, proving regulatory compliance to auditors is greatly simplified when entitlements are managed at the business role level. After business roles have been defined, proving compliance becomes a simple matter of verifying that users are assigned the appropriate business roles.

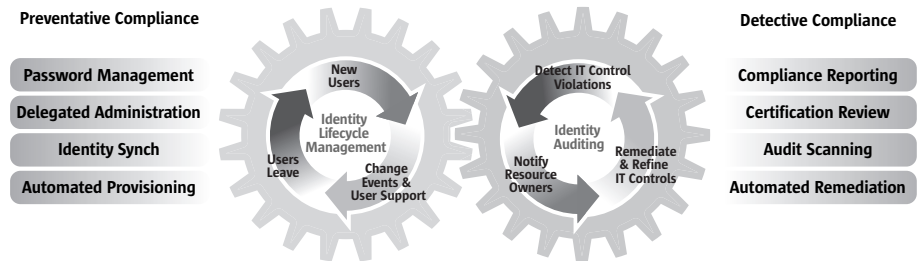


Figure 1. Converged provisioning and identity auditing reduces the risk of non-compliance by creating a continuous audit cycle, which makes it possible to detect and prevent compliance violations in an ongoing, sustainable manner.

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, auditing, and role management solution specifically reduces compliance costs by also automating identity auditing, which many companies still handle manually, and by further streamlining the provisioning and auditing processes. This streamlining creates greater efficiencies, which helps increase productivity and reduce the costs traditionally associated with provisioning and auditing.

Recertification — the quarterly process where managers approve direct reports' access to enterprise resources and applications — is an excellent example of where role management can reduce costs. With manual recertification, approving managers often waste time trying to understand a raw list of IT entitlements assigned to their direct reports. Understanding AD groups and LDAP directories is not a critical job function for most approving managers, and tracking this information down once a quarter is a waste of time and money. Also, when approving managers grant carte blanche access to users' entitlements, they increase the risk of SOD violations — and regulatory fines as the result of failing an audit.

A role management solution greatly reduces the likelihood of these unwanted outcomes. By performing a recertification with entitlements represented to the approving manager at the business role level, the manager can attest to those entitlements quickly and accurately because they are given in a meaningful business context.

Further automating the provisioning process

Without a role management solution, automated provisioning can only increase efficiencies by so much. Compliant provisioning through a single platform with integrated workflow for approvals provides significant benefits over a manual approach; however, adding role management to the equation greatly enhances these benefits. This is best illustrated through an onboarding example. Without role management, a new employee or user must be assigned raw IT entitlements that may have little business context. Uncertainty regarding appropriate entitlements increases the time it takes to onboard the new employee.

This uncertainty is mitigated with a role management solution. Approving managers only need to know that the new user has been assigned the appropriate business roles or job title, thus eliminating the need to understand raw IT entitlements before granting approval for a particular resource or application.

Chapter 4

Using Sun's Integrated Role Management Solution to Meet Major Business Objectives

Sun Identity Manager software, combined with Sun Role Manager technology, is the only truly integrated solution that addresses provisioning and auditing at the business role level. Its capabilities specifically enable companies to meet three major business objectives: compliance, cost control, and automated provisioning.

- **Role management**

Sun Identity Manager software enables provisioning and auditing at the business role level, increasing efficiencies and providing greater controls over the provisioning and auditing processes. Integration with Sun Role Manager technology ensures Sun Identity Manager software can consume predefined roles that can be used for provisioning and auditing.

- **Role definition and discovery**

Sun Role Manager software is the only role product that approaches role mining and definition from the top down and the bottom up. This combined approach ensures that roles are defined appropriately for the needs of the organization and helps prevent role explosion.

- **Complete visibility into current compliance exposures**

Sun Identity Manager software'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 Sun Identity Manager software. In addition, the solution provides reports on policy violations, remediations, and exceptions and enables custom reports of audit data.

- **Scalable provisioning and identity auditing for extranet-facing environments**

With Sun Identity Manager software, companies have a scalable option in extranet-facing applications and portals. The solution's extranet and federated identity administration capabilities can help introduce more 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 Role Management

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

Scenario 1: Ensuring segregation of duties at a large manufacturing company

Situation: Maria, an accountant working in the Accounts Receivable group, takes the opportunity to move to another group within the company, where she will work in the Accounts Payable department. 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 SOD 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 SOD.

Solution: The company deploys Sun Identity Manager software, which automates provisioning and identity auditing at the business role level. Using roles defined in Sun Role Manager software, an employee who leaves one area to join another can be provisioned for new responsibilities instantly by assigning the employee a new business role; the employee can also be automatically deprovisioned for resources associated with the previous position by removing the old business role. This eliminates the risk of violating Sarbanes-Oxley requirements requiring SOD and prohibiting erroneous aggregation of privileges.

Scenario 2: Automating recertification at a major insurance company

Situation: A major insurance 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 and compliant. This is done manually by generating reports and sending them to users' managers and application owners to review and approve. Because of the large 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 their certification review process by implementing Sun Identity Manager software to automatically track approvals, notify managers when it's time for a review, and escalate when reviewers fail to respond. This process is further streamlined by performing access reviews at the business role level instead of reviewing and approving raw lists of IT entitlements. Sun Identity Manager software also generates reports that capture all approvals and document all remediations for auditing purposes. By automating processes in order to dramatically streamline access review, Sun Identity Manager software 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 Sun Identity Manager software. The solution's combined provisioning, auditing, and role management 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, that employee's HR benefits role will be deprovisioned and a new role will be assigned based on the new job.

Chapter 6

Conclusion

A robust IAM solution that provides capabilities for provisioning, auditing, and role management is paramount to helping companies achieve regulatory compliance at a reasonable cost. The efficiencies and greater controls introduced by combining automated provisioning and auditing into a single solution are greatly enhanced by seamless integration with role management capabilities. By managing the provisioning and auditing processes at the business role level, companies can ensure continuous compliance while reducing costs and staying competitive.

To learn more about Sun's complete identity and role management solution, visit www.sun.com/identity.

