

The Role of Identity Management in Sarbanes-Oxley Compliance

A Business White Paper
September 2004



Table of Contents

Executive Summary	1
Sarbox Compliance and Information Technology's Role	2
Identity Management Addresses Sarbox "Adequate Internal Controls"	3
Sun Identity Management and Sarbox Compliance	4
Conclusion	9

Chapter 1

Executive Summary

Thanks to the Sarbanes-Oxley Act (Sarbox), the U.S. government's response to several well-publicized corporate financial scandals (Enron, WorldCom, Adelphia, Tyco, and others), strong corporate governance practices and a business code of ethics are not just good corporate etiquette — they are the law. Essentially, the government is requiring that CEOs and CFOs of public companies swear under oath that the financial statements they make are accurate and complete. The purpose of the act is to protect investors by improving the reliability of corporate financial statements and establishing stiffer penalties for auditors, corporate officers, company directors, and others who violate the act.

The impact of Sarbox since it was signed into law on July 30, 2002 has been significant and far-reaching. Essentially, every publicly traded company, big or small, domestic or foreign, that has registered under the Exchange Act or has a pending registration statement under the Securities Act of 1933 is affected by this legislation. Failure to comply with Sarbox requirements carries significant penalties, including jail terms for executives and corporate fines.

“Companies are seriously concerned that they don't have the appropriate internal controls and financial management processes in place to comply with Sarbox. In fact, almost 90 percent of the companies surveyed are already engaged in evaluating or implementing a Sarbox project, and 40 percent intend to upgrade current processes and systems in their compliance efforts.”

– John Van Decker, Vice President, Technology Research Services of META Group — Comments on a survey conducted by PeopleSoft, with results analyzed by META Group — December 2003, e-Week

Chapter 2

Sarbox Compliance and Information Technology's Role

According to an extensive study of enterprise compliance strategies released by META Group, Inc. on July 27, 2004, “about 64 percent of all public companies currently have budgets dedicated to financial regulatory compliance, with the average budget projected to be \$7.2 million in 2005. Among those companies without a current budget, more than half (54 percent) plan to allocate money for compliance initiatives within the next 12 months.”

While Sarbox is not detailed in prescribing a solution to the compliance issue, it does make clear what obligations the company is under in order to be compliant. Explicitly, section 404(a) of the act requires establishing “adequate internal controls” around financial reporting and its governance. The “internal controls” that Sarbox refers to ultimately break down into a series of processes that companies must adhere to in the preparation of financial reports, as well as the protection of the financial information — that goes into making the reports — as it is stored in various locations throughout the enterprise (including enterprise applications, database tools, and even in accounting spreadsheets).

IT and its related processes generate the majority of data that makes up financial reports, therefore, it is critical that the effectiveness of these processes can be verified. Sun believes that IT plays a critical part in ensuring its company is in compliance with Sarbox. If not, the risk to the corporation and potential personal liability to executives can be significant.

Identity management plays a significant part in IT's larger plan for Sarbox compliance. This paper will discuss the role that identity management plays in the protection of this financial information so that CEOs and CFOs can be confident that the reports they are certifying come from well-maintained, secure, and error-free software applications and processes.

Chapter 3

Identity Management Addresses Sarbox “Adequate Internal Controls”

According to AMR Research¹, many companies feel that Sarbox requires a holistic look at business and IT infrastructure, starting with financial processes and reaching back to the operational processes that promote them. Any investments made towards Sarbox compliance should also improve the business and provide a return on investment (ROI).

When it comes to system security and the control of access to systems and applications, Sarbox is not explicitly prescriptive. It does not articulate what “adequate internal controls” means, or what solutions an organization must implement in order to affect them. However, by drawing from industry best practices for security and control of other types of information, several inferences can be made.

A quick review of the Sarbox legislation reveals the following common requirements for internal control:

- 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 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 put in place — including the elimination of multiple user IDs and accounts for individual persons.
- The allocation of passwords should be 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.

Each of these requirements can be specifically addressed by a comprehensive enterprise identity management solution.

1. *Sarbox Compliance: An AMR Research Guide and Framework*, John Hagerty, AMR Research, September 15, 2003.

Chapter 4

Sun Identity Management and Sarbox Compliance

Sun enables Sarbox compliance by providing everything an enterprise needs to securely and efficiently manage identities and their access to sensitive data and systems, including:

- User provisioning/deprovisioning
- Password management
- Access management
- Account management and self-service
- Activity monitoring, auditing, and reporting
- Directory management

Sun provides the industry's most innovative and comprehensive portfolio for using, sharing, and managing identity information. Sun's identity management suite include three products that are critical to the success of any identity management solution:

- **Sun Java™ System Identity Manager** is a noninvasive and secure user provisioning and data synchronization solution that uses automation and delegation to reduce the time and costs associated with enabling new users to start working productively and instantly disabling access when relationships change or end for a more secure enterprise. Java System Identity Manager also provides a complete password management solution that enables end users to manage their passwords themselves, increasing their satisfaction while greatly reducing associated support costs.
- **Sun Java System Access Manager** provides decentralized authentication and authorization services across internal and external computing domains and ensures that appropriate authentication credentials are required of users depending on the value of the protected resources. Java System Access Manager makes certain that authorized users have access to specific resources while simultaneously protecting those resources from unauthorized users. It presents streamlined navigation across enterprise Web applications through single sign-on capabilities, and also enables the enterprise to audit all access activities, including authentication attempts, authorizations, and changes made, to assist in complying with regulatory audit requirements.
- **Sun Java System Directory Server Enterprise Edition** delivers secure, highly available, and scalable directory services for storing and managing accurate and reliable identity data. It serves as the backbone to an enterprise identity infrastructure, enabling today's mission-critical enterprise applications and large-scale extranet applications to access consistent, accurate, and reliable identity data for significant operational and cost efficiencies. Java System Directory Server Enterprise Edition integrates smoothly into multiplatform environments, and provides secure, on-demand password synchronization with Microsoft Windows Active Directory.

Sun's identity management products enable Sarbox compliance in the following areas:

	User Provisioning & Termination	Password Management	Access Management	Account Management & Self-Service	Activity Monitoring & Auditing	Directory Management & Service
Identity Manager	X	X	X	X	X	X
Access Manager	X	X	X		X	X
Directory Server Enterprise Edition		X		X	X	X

For Sarbox compliance, Sun's identity management solution not only allows secure control over the access to and use of information systems, it provides key components such as user provisioning/deprovisioning, access management, password management, account management, directory management, and robust monitoring, audit, and reporting.

Sun's identity management solution can directly address each of the Sarbox implications and help with compliance as highlighted in the following chart:

Regulation Implication	Sun's Identity Management Capabilities
1. Financial reports must be verifiable and auditable: This implies that IT must provide assurance that a company's mission-critical software applications are not exposed to potential failure due to human error, staff turnover, or sabotage.	<ul style="list-style-type: none"> • User and privilege management. Identity Manager provides complete and centralized visibility into access privileges, for control and up-to-the minute insight into who has access to what resources and information throughout the enterprise. This control ensures that only the right people have access to sensitive financial information and applications that provide the basis of financial reporting. This level of control helps to ensure that the integrity of the information stored in these systems is not subject to accidental contamination or malicious manipulation.
	<ul style="list-style-type: none"> • Elimination of orphan accounts. With active risk scanning, Identity Manager automatically scans for orphan or dormant accounts that may pose a security risk. These accounts can then be eliminated, if necessary, to provide an accurate picture of the enterprise's activities.
	<ul style="list-style-type: none"> • Access management. Access Manager provides a standards solution for secure and scalable access to resources within and across federated business networks. Access Manager makes certain that authorized users have access to specific resources while protecting those resources from unauthorized users. <p>By utilizing a central point of authentication and role- and rule-based access control, Access Manager ensures that security policies can be centrally enforced, resulting in improved security and simplified management. Access Manager keeps track of intrusions and unauthorized access activity with real-time audit of any such events. It also creates well-defined, repeatable, and auditable security processes that can be enforced enterprise-wide based on user identities.</p>

Regulation Implication	Sun's Identity Management Capabilities
	<p>• Directory management. Directory Server Enterprise Edition provides firewall-like protection against malicious attempts to compromise directory servers. It serves as a front end to prevent denial-of-service (DoS) attacks and access by unauthorized users.</p> <p>In order to comply with Sarbox, information and systems must be reliable and highly available such that reports and real-time audits can access data without gaps or time lapses. Directory Server Enterprise Edition provides the backbone to an enterprise identity infrastructure that is reliable and highly available. With load balancing and failover/failback, it provides seamless operations and minimal interruptions for enterprise environments.</p>
	<p>• Password management and policy enforcement. Password policies play an integral role in ensuring the integrity of an enterprise's security program by restricting access to only authorized personnel. However, password management can be complicated when there are diverse relationships between users and the systems and applications they are trying to access.</p> <p>Sun's identity management products make it easier for users to manage their passwords and administrators to enforce password policies. Users benefit from the ability to synchronize the passwords they use for a variety of resources and applications they are trying to access. And administrators benefit from an automated, secure access system that gives them a centralized location for password policy enforcement.</p>
<p>2. Real-time disclosure: Requires "timely and accurate disclosure of material events" to the business. Implies that companies must be ready to disclose events that affect the business within 48 hours.</p>	<p>• Real-time audit and reporting. Identity Manager offers comprehensive audit and reporting on profile data, change history, and user permissions enterprise-wide. It detects security risks and alerts administrators to respond.</p> <p>• Activity monitoring. By providing current and accurate reports of who is allowed access to what information and why, with the ability to adjust those access levels, Identity Manager addresses the requirement of management authorization for employee activities. This is a key component of the report filing and accountability maintenance requirements under Sarbox and its references to the Securities Exchange Act of 1934.</p> <p>Furthermore, reports reflecting changes to authorized access may be generated and automatically sent to managers at predefined intervals. This enables administrators to compare previous and/or current access records and make the changes necessary to preserve the required knowledge of accountability within the enterprise.</p>

Regulation Implication	Sun's Identity Management Capabilities
	<ul style="list-style-type: none"> • Auditing and reporting. Identity Manager enables administrators to see instantly who has access to what and why, with current, accurate views and reports of user access privileges on IT resources as well as administrative privileges on key systems. Identity Manager will also review the status of access privileges for any given date in the past; it stores access data for as long as required. With Identity Manager, access data can be retained as long as necessary for the review of access history and user accountability. Access privileges related to specific dates can be recovered and studied for periodic reports or upcoming information security audits. <p>Real-time audit is possible with Access Manager as well. It provides up-to-the-minute auditing of all authentication attempts, authorizations, and changes made. With real-time audit capability, Access Manager improves security and internal control by providing instant auditing of critical information.</p> <p>Directory Server Enterprise Edition provides audit logging, which can be used to determine who accessed what and when. It also includes scripts that process these logs to create reports.</p>
<p>3. Auditability of the internal control structure and processes: Requires that companies demonstrate appropriate levels of enforcement of business processes involved in financial reporting.</p>	<ul style="list-style-type: none"> • Secure business-to-business (B2B) collaboration. Access Manager makes it possible for an authenticated identity to be recognized and for the authorized user associated with that identity to securely access financial information based on their job functions across multiple domains. <p>Within the enterprise, a federated identity strategy can be implemented to allow employees to seamlessly and securely access multiple financial applications without interruption. By utilizing a central point of authentication and role- and rule-based access control, Access Manager ensures that security policies are centrally enforced, and that the right level of resource protection for a given resource is used. These centralized authentication and authorization services enhance and consistently apply security policies as required.</p>
	<ul style="list-style-type: none"> • Rules engine. Identity Manager enforces business rules by automatically completing access privilege changes according to corporate policies. • Role- and rule-based access control. Through the use of role-based access control (RBAC), combined with a flexible rules-based model, Identity Manager ensures that only appropriate levels of access to financial information are given to individuals based on their job functions and responsibilities. Instead of managing the access privileges of individuals on a one-off basis — a task that is often insurmountable from a workload effort — Identity Manager uses role and rule-based access controls to allow organizations to manage permissions on group level. This provides a highly scalable and streamlined mechanism for turning access privileges on and off as individuals enter, leave, and transition jobs within the organization.
	<ul style="list-style-type: none"> • Dynamic workflow and approval processes. Within the specified enterprise business processes, Identity Manager securely automates the process of changing access permissions such as approvals and notifications. This is conducted as business rules and security policies are encoded into the workflow process, ensuring that access privilege changes are undertaken according to corporate policies each and every time. The workflows are completely enforceable, meaning that a process cannot be subverted by an overzealous or malicious employee who wishes to skip steps in the process.

Regulation Implication	Sun's Identity Management Capabilities
	<ul style="list-style-type: none"> • Fine-grained access control. Directory Server Enterprise Edition ensures compliance through its ability to deny or allow access based on IP address, group membership, and other criteria.
	<ul style="list-style-type: none"> • Enforcement of unique user IDs. When Identity Manager is deployed, a unique identifier is assigned to each individual with access privileges to any enterprise resource (network, database, applications, etc.). This unique identifier is mapped to the various distributed accounts owned by that individual, ensuring that each individual is effectively “tracked” with respect to access privileges and that no one individual has multiple access points into any one data store or application. All access points are effectively and completely disabled when it is no longer appropriate for an individual to hold them.
<p>4. Extend beyond the usual financial systems. This has implications of not only regulating basic financial applications and systems, but also enterprise resource planning (ERP), customer relationship management (CRM), and supply chain management (SCM) applications (because they are involved in business and financial transactions at some level).</p>	<ul style="list-style-type: none"> • Broad platform support. Sun's identity management solutions are designed to integrate seamlessly across heterogeneous enterprise IT environments — from mainframe and business applications to the latest Web applications and portals.
	<ul style="list-style-type: none"> • Federation support. Because it is difficult for enterprises to forecast which systems and solutions their company will implement in the future, it is critical that their identity management vendor delivers support for the current and latest standards, and takes a strong role in creating future standards. Access Manager supports the latest federation standards and provides interoperability across different vendor platforms, protecting enterprises' existing technology investments. It also allows organizations to protect the privacy and security of their financial information while providing the ability to integrate business applications and linking the access to these applications across divisions or business networks. <p>Sun is leading the industry in providing fully productized support for the latest federation standards providing interoperability and meeting regulatory compliance. Access Manager support of the latest federation standards, including Liberty Alliance ID-WSF and SAML 1.1 specifications, helps create a federated framework sharing mechanism that is secure, interoperable, and easy to use with existing enterprise applications.</p>

Chapter 5

Conclusion

Compliance with Sarbox can be a time-consuming, difficult, and expensive effort. Organizations will attempt their initial compliance within the framework of their existing technology and procedures. However, compliance with Sarbox requires more than just updating processes and documentation to ensure the integrity of financial data. “Management must continue to evaluate and test their internal controls over financial reporting across all business units and functional areas as risk factors evolve over time. While Sarbox doesn’t specify which measures to take to mitigate risks introduced by control weakness, the use of strong technical safeguards to enhance the control environment is critical.”² As part of its identity management solutions, Sun provides significant capabilities that directly impact Sarbox compliance issues and enhance and secure these internal controls.

With the passing of the Sarbox Act, the government has issued a call to action for corporate America. Under its mandates, failure for public companies to comply can result in serious consequences, including fines, sanctions, and in cases of severe negligence, jail terms for corporate executives and board members. Implementing an end-to-end identity management solution effectively addresses the compliance requirements associated with internal control of access rights and entitlements to the data and applications that feed financial reporting processes. Conversely, the lack of an effective identity management infrastructure makes it virtually impossible to assure that financial reporting is based on reliable and verified information.

Sun is the market leader in providing Fortune 1000 companies and service providers with identity management solutions that address these internal controls. With proven technology and an innovative architecture that assures near-term results, Sun is leading the way in helping companies meet Sarbox compliance.

For more information, visit sun.com/identity_mgmt.

© 2004 Sun Microsystems, Inc., 4150 Network Circle, Santa Clara, CA 95054 USA

All rights reserved.

This product or document is protected by copyright and distributed under licenses restricting its use, copying, distribution, and decompilation. No part of this product or document may be reproduced in any form by any means without prior written authorization of Sun and its licensors, if any. Third-party software, including font technology, is copyrighted and licensed from Sun suppliers.

Parts of the product may be derived from Berkeley BSD systems, licensed from the University of California.

Sun, Sun Microsystems, the Sun logo, Java, and The Network is the Computer are trademarks, registered trademarks, or service marks of Sun Microsystems, Inc. in the U.S. and other countries.

UNIX is a registered trademark in the United States and other countries, exclusively licensed through X/Open Company, Ltd.

All SPARC trademarks are used under license and are trademarks or registered trademarks of SPARC International, Inc. in the U.S. and other countries. Products bearing SPARC trademarks are based upon an architecture developed by Sun Microsystems, Inc.

The OPEN LOOK and Sun™ Graphical User Interface was developed by Sun Microsystems, Inc. for its users and licensees. Sun acknowledges the pioneering efforts of Xerox in researching and developing the concept of visual or graphical user interfaces for the computer industry. Sun holds a non-exclusive license from Xerox to the Xerox Graphical User Interface, which license also covers Sun's licensees who implement OPEN LOOK GUIs and otherwise comply with Sun's written license agreements.

RESTRICTED RIGHTS: Use, duplication, or disclosure by the U.S. Government is subject to restrictions of FAR 52.227-14(g)(2)(6/87) and FAR 52.227-19(6/87), or DFAR 252.227-7015(b)(6/95) and DFAR 227.7202-3(a). DOCUMENTATION IS PROVIDED "AS IS" AND ALL EXPRESS OR IMPLIED CONDITIONS, REPRESENTATIONS AND WARRANTIES, INCLUDING ANY IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT, ARE DISCLAIMED, EXCEPT TO THE EXTENT THAT SUCH DISCLAIMERS HELD TO BE LEGALLY INVALID.



Please
Recycle



Adobe PostScript

Sun Microsystems, Inc. 4150 Network Circle, Santa Clara, CA 95054 USA Phone 1-650-960-1300 or 1-800-555-9SUN Web sun.com



Sun Worldwide Sales Offices: Argentina +5411-4317-5600, Australia +61-2-9844-5000, Austria +43-1-60563-0, Belgium +32-2-704-8000, Brazil +55-11-5187-2100, Canada +905-477-6745, Chile +56-2-3724500, Colombia +571-629-2323, Commonwealth of Independent States +7-502-935-8411, Czech Republic +420-2-3300-9311, Denmark +45 4556 5000, Egypt +202-570-9442, Estonia +372-6-308-900, Finland +358-9-525-561, France +33-134-03-00-00, Germany +49-89-46008-0, Greece +30-1-618-8111, Hungary +36-1-489-8900, Iceland +354-563-3010, India-Bangalore +91-80-2298989/2295454; New Delhi +91-11-6106000; Mumbai +91-22-697-8111, Ireland +353-1-8055-666, Israel +972-9-9710500, Italy +39-02-641511, Japan +81-3-5717-5000, Kazakhstan +7-3272-466774, Korea +822-2193-5114, Latvia +371-750-3700, Lithuania +370-729-8468, Luxembourg +352-49 11 33 1, Malaysia +603-21161888, Mexico +52-5-258-6100, The Netherlands +00-31-33-45-15-000, New Zealand-Auckland +64-9-976-6800; Wellington +64-4-462-0780, Norway +47 23 36 96 00, People's Republic of China-Beijing +86-10-6803-5588; Chengdu +86-28-619-9333, Guangzhou +86-20-8755-5900; Shanghai +86-21-6466-1228; Hong Kong +852-2202-6688, Poland +48-22-8747800, Portugal +351-21-4134000, Russia +7-502-935-8411, Saudi Arabia +9661 273 4567, Singapore +65-6438-1888, Slovak Republic +421-2-4342-94-85, South Africa +27 11 256-6300, Spain +34-91-767-6000, Sweden +46-8-631-10-00, Switzerland-German 41-1-908-90-00; French 41-22-999-0444, Taiwan +886-2-8732-9933, Thailand +662-344-6888, Turkey +90-212-335-22-00, United Arab Emirates +9714-3366333, United Kingdom +44 0 1252 420000, United States +1-800-555-9SUN or +1-650-960-1300, Venezuela +58-2-905-3800, or online at sun.com/store

SUN © 2004 Sun Microsystems, Inc. All rights reserved. Sun, Sun Microsystems, the Sun logo, Java, and The Network is the Computer are trademarks or registered trademarks of Sun Microsystems, Inc. in the United States and other countries. Information subject to change without notice. 09/04 R1.0